特　許　協　力　条　約

EP ・ US　PCT

国際調査報告

（法８条、法施行規則第40、41条）
〔ＰＣＴ１８条、ＰＣＴ規則43、44〕

出願人又は代理人の書類記号　520269W001	今後の手続きについては、国際調査報告の送付通知様式（ＰＣＴ／ＩＳＡ／２２０）及び下記５を参照すること。	
国際出願番号 ＰＣＴ／ＪＰ００／００４７４	国際出願日（日.月.年）　２８．０１．００	優先日（日.月.年）
出願人（氏名又は名称）　三菱電機株式会社		

国際調査機関が作成したこの国際調査報告を法施行規則第41条（ＰＣＴ１８条）の規定に従い出願人に送付する。
この写しは国際事務局にも送付される。

この国際調査報告は、全部で　2　ページである。

☐ この調査報告に引用された先行技術文献の写しも添付されている。

１．国際調査報告の基礎

ａ．言語は、下記に示す場合を除くほか、この国際出願がされたものに基づき国際調査を行った。
☐ この国際調査機関に提出された国際出願の翻訳文に基づき国際調査を行った。

ｂ．この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際調査を行った。
☐ この国際出願に含まれる書面による配列表
☐ この国際出願と共に提出されたフレキシブルディスクによる配列表
☐ 出願後に、この国際調査機関に提出された書面による配列表
☐ 出願後に、この国際調査機関に提出されたフレキシブルディスクによる配列表
☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった。
☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記録した配列が同一である旨の陳述書の提出があった。

２．☐ 請求の範囲の一部の調査ができない（第Ｉ欄参照）。

３．☐ 発明の単一性が欠如している（第Ⅱ欄参照）。

４．発明の名称は
☑ 出願人が提出したものを承認する。
☐ 次に示すように国際調査機関が作成した。

５．要約は
☑ 出願人が提出したものを承認する。
☐ 第Ⅲ欄に示されているように、法施行規則第47条（ＰＣＴ規則38.2(b)）の規定により国際調査機関が作成した。出願人は、この国際調査報告の発送の日から１カ月以内にこの国際調査機関に意見を提出することができる。

６．要約書とともに公表される図は、
第　2　図とする。☑ 出願人が示したとおりである。　☐ なし
☐ 出願人は図を示さなかった。
☐ 本図は発明の特徴を一層よく表している。

国際調査[redacted]　　国際出願番[redacted] PCT／JP00／00474

A.　発明の属する分野の分類（国際特許分類（IPC））
Int.Cl⁷
H04L　9／08
H04L　29／02

B.　調査を行った分野
調査を行った最小限資料（国際特許分類（IPC））
Int.Cl⁷
G09C　1／00 － 5／00　　H04K　1／00 － 3／00
H04L　9／00　　H04L　29／00

最小限資料以外の資料で調査を行った分野に含まれるもの

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）
JICSTファイル（JOIS）
INSPEC（DIALOG）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	Paul Albits and Criket Liu, 高田広章，小島育夫監訳，小舘光正訳，「DNS & BIND 第3版」第2版，オライリー・ジャパン，(1999年6月3日)，pp. vii－ix，100－102	1-12
Y	RFC (Request for Comments) 2065, D. Eastlake, 3rd and C. Kaufman, "Domain Name System Security Extensions," (Jan 1997)	1-12
A	RFC (Request for Comments) 1035, P. Mockapetris, "DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION," (Nov 1987)	1-12

☐ C欄の続きにも文献が列挙されている。　　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
13.04.00	25.04.00

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	
日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	丸山　高政	5W　9570
	電話番号　03－3581－1101　内線　9570	

様式PCT／ISA／210（第2ページ）（1998年7月）

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2001年8月2日 (02.08.2001)

PCT

(10) 国際公開番号
WO 01/56223 A1

(51) 国際特許分類[7]: H04L 9/08, 29/02

(21) 国際出願番号: PCT/JP00/00474

(22) 国際出願日: 2000年1月28日 (28.01.2000)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人 (米国を除く全ての指定国について): 三菱電機株式会社 (MITSUBISHI DENKI KABUSHIKI KAISHA) [JP/JP]; 〒100-8310 東京都千代田区丸の内二丁目2番3号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 武田紀子 (TAKEDA, Noriko) [JP/JP]; 〒100-0006 東京都千代田区有楽町一丁目12番1号 三菱電機システムウエア株式会社内 Tokyo (JP). 笹本明彦 (SASAMOTO, Akihiko) [JP/JP]. 足立一幸 (ADACHI, Kazuyuki) [JP/JP]. 篠田誠一 (SHINODA, Seiichi) [JP/JP]; 〒100-8310 東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内 Tokyo (JP).

(74) 代理人: 溝井章司, 外(MIZOI, Shoji et al.); 〒247-0056 神奈川県鎌倉市大船二丁目17番10号 NTA大船ビル 3F Kanagawa (JP).

(81) 指定国 (国内): CA, IL, JP, US.

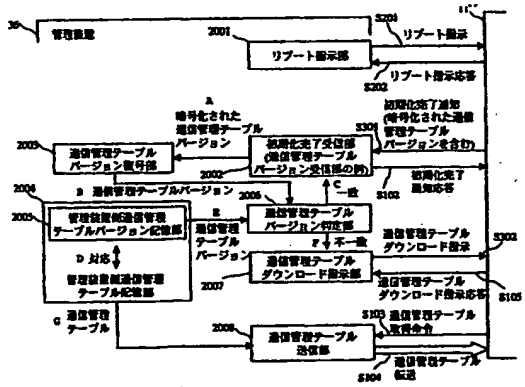
(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(54) Title: COMMUNICATION MANAGING TABLE TRANSFER SYSTEM AND MANAGING DEVICE, CIPHERING DEVICE, AND COMMUNICATION MANAGING TABLE TRANSFER METHOD

(54) 発明の名称: 通信管理テーブル転送システム及び管理装置及び暗号装置及び通信管理テーブル転送方法



36...MANAGING DEVICE
2001...REBOOT INSTRUCTING SECTION
S201...REBOOT INSTRUCTION
S202... RESPONSE TO REBOOTING INSTRUCTION
2003...COMMUNICATION MANAGING TABLE VERSION DECODING SECTION
B...COMMUNICATION MANAGING TABLE VERSION
A...CIPHERED COMMUNICATION MANAGING TABLE VERSION
2002...INITIALIZATION END RECEIVING SECTION (EXAMPLE OF COMMUNICATION MANAGING TABLE VERSION RECEIVING SECTION)
S302...NOTIFICATION OF INITIALIZATION END (CONTAINING CIPHERED COMMUNICATION MANAGING TABLE VERSION)
S102...RESPONSE TO NOTIFICATION OF INITIALIZATION END
2004...COMMUNICATION MANAGING TABLE STORAGE SECTION ON MANAGING DEVICE SIDE
2005... COMMUNICATION MANAGING TABLE VERSION STORAGE SECTION ON MANAGING DEVICE SIDE
D...CORRESPONDENCE
C...COMMUNICATION MANAGING TABLE
E...COMMUNICATION MANAGING TABLE VERSION
2006...COMMUNICATION MANAGING TABLE VERSION JUDGING SECTION
G...AGREEMENT
F...DISAGREEMENT
2007...COMMUNICATION MANAGING TABLE DOWNLOARD INSTRUCTING SECTION
2008...COMMUNICATION MANAGING TABLE TRANSMITTING SECTION
S302...COMMUNICATION MANAGING TABLE DOWNLOAD INSTRUCTION
S105...RESPONSE TO COMMUNICATION MANAGING TABLE DOWNLOAD INSTRUCTION
S103...COMMUNICATION MANAGING TABLE ACQUISITION INSTRUCTION
S104...COMMUNICATION MANAGING TABLE TRANSFER

(57) Abstract: A communication managing table transfer system comprising ciphering devices interconnected through an internet, a managing device for managing a communication managing table used for communication by the ciphering devices, providing improved security, and having improved performance. A managing device (36) receives a communication managing table version from a ciphering device (11) (S301), a communication managing table version judging section

/続葉有/

WO 01/56223 A1

(2006) compares the received communication table version with the communication managing table version stored in a communication managing table version storage section (2005) on the managing device side and transfers the communication managing table to the cipher device (11) only if the result of the comparison shows that both disagree with each other (S104).

(57) 要約:

インターネットを介して互いに接続する複数の暗号装置と、上記複数の暗号装置が通信に用いる通信管理テーブルを管理する管理装置とからなる通信管理テーブル転送システムに係り、セキュリティの向上と、性能の向上とを図ることを課題とする。

管理装置３６は、暗号装置１１から通信管理テーブルバージョンを受信し（Ｓ３０１）、通信管理テーブルバージョン判定部２００６で、管理装置側通信管理テーブルバージョン記憶部２００５に記憶している通信管理テーブルバージョンと比較し、不一致の場合にのみ暗号装置１１に対して通信管理テーブルを転送する（Ｓ１０４）。

明　細　書

通信管理テーブル転送システム及び管理装置及び暗号装置及び通信管理テーブル転送方法

技術分野

本発明は、インターネットを介して互いに接続する複数の暗号装置と、上記複数の暗号装置が通信に用いる通信管理テーブルを管理する管理装置とからなる通信管理テーブル転送システムに係り、セキュリティの向上と、性能の向上に関する。

背景技術

近年、仮想私設網（ＶＰＮ：Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）を用いるシステムが普及している。仮想私設網は、データの暗号化やユーザ認証などのセキュリティ技術を用いてインターネット等のパブリックネットワークを仮想的（Ｖｉｒｔｕａｌ）に専用線（Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）のように利用するネットワークのことである。仮想私設網によって、複数の組織における内部ネットワーク間を専用線を用いるかのごとく接続することができる。

図１３は、仮想私設網を用いるシステムの例を示す図である。１は、インターネット、１１、２１、３１は、暗号装置、１２、２２、３２は、ルータ、１３、２３、３３は、ファイアウォール、１４、２４、３４は、サブネット（内部ネットワーク）、１５、２５、３５は、通信端末、３６は、管理装置である。それぞれ、図のように接続されている。

インターネットを介したデータ転送を行なう場合、外部からの攻撃に対する防御手段としてＩＰ　ｓｅｃｕｒｕｔｙに準拠するシステムが用

いられる。ＩＰ　ｓｅｃｕｒｕｔｙは、インターネット通信規約標準化機関ＩＥＴＦ（Ｉｎｔｅｒｎｅｔ　Ｅｎｇｉｎｅｅｒｉｎｇ　Ｔａｓｋ　Ｆｏｒｃｅ）で定められたＩＰパケットレベルにおけるセキュリティ確保方式のことである。

ＩＰ　ｓｅｃｕｒｕｔｙでは、各内部ネットワーク上の暗号装置間で、ＳＡ（Ｓｅｃｕｒｉｔｙ　Ａｓｓｏｃｉａｔｉｏｎ）という関係を確立した上で、データの転送を行なう。これにより、秘匿通信が可能となる。しかし、ＳＡを確立する為には、その前提として公開鍵を暗号装置間で共有化しておく必要がある。

また、内部ネットワーク上の通信端末に対してデータを転送する場合には、各内部ネットワークの構成情報を知っておく必要もある。

そのため、上記の公開鍵や内部ネットワークの構成情報を含む通信管理テーブルを生成し、ＳＡの確立の前にこの通信管理テーブルを暗号装置間で交換する。このような通信管理テーブルを作成し、更新し、配信するために管理装置３６が設置される。

従来、暗号装置から通信管理テーブルを求められた管理装置３６は、無条件に通信管理テーブルを暗号装置へ配信していた。

図１４は、従来例における電源を入れたときの通信管理テーブルの転送の手順を示す図である。暗号装置Ａ１１の電源がいれられると、暗号装置Ａ１１は、暗号装置初期化通知（Ｓ１０１）を送信する。管理装置３６は、暗号装置初期化通知（Ｓ１０１）を受信すると、暗号装置初期化通知応答（Ｓ１０２）を送信する。暗号装置Ａ１１は、暗号装置初期化通知応答（Ｓ１０２）を受信すると無条件に通信管理テーブル取得命令（Ｓ１０３）を発行し、通信管理テーブル転送（Ｓ１０４）が行なわれる。

また、図１５は、従来例におけるリブートされたときの通信管理テー

ブルの転送の手順を示す図である。管理装置３６が、リブート指示（Ｓ２０１）を送信し、暗号装置Ａ１１が、リブート指示応答（Ｓ２０２）を送信した後、再起動する。これ以降、図１４と同様に動作する。

上述のシステムにおいては、通信管理テーブルの転送回数が多く、データ転送の性能を劣化させていた。

また、通信管理テーブルを盗用される機会を増加させ、セキュリティ上の問題があった。つまり、公開鍵や内部ネットワークの構成情報を盗まれ、暗号装置間のデータ転送の秘匿が守られないおそれがあった。

本発明は、上記した従来技術の欠点を除くためになされたものであって、通信管理テーブルの転送回数を減らし、データ転送の性能を向上させ、通信管理テーブルを盗用される機会を減らし、セキュリティを向上させることを目的とする。

発明の開示

この発明に係る通信管理テーブル転送システムは、インターネットを介して互いに接続する複数の暗号装置と、上記複数の暗号装置が通信に用いる通信管理テーブルを管理する管理装置とからなる通信管理テーブル転送システムであって、

上記暗号装置は、上記暗号装置で記憶する上記通信管理テーブルである暗号装置側通信管理テーブルを記憶する暗号装置側通信管理テーブル記憶部と、

上記暗号装置側通信管理テーブルのバージョンである暗号装置側通信管理テーブルバージョンを記憶する暗号装置側通信管理テーブルバージョン記憶部と、

上記暗号装置側通信管理テーブルバージョンを、上記管理装置へ送信する通信管理テーブルバージョン送信部とを備え、

上記管理装置は、上記管理装置で記憶する上記通信管理テーブルである管理装置側通信管理テーブルを記憶する管理装置側通信管理テーブル記憶部と、

上記管理装置側通信管理テーブルのバージョンである管理装置側通信管理テーブルバージョンを記憶する管理装置側通信管理テーブルバージョン記憶部と、

上記暗号装置から上記暗号装置側通信管理テーブルバージョンを受信する通信管理テーブルバージョン受信部と、

受信した上記暗号装置側通信管理テーブルバージョンと、上記管理装置側通信管理テーブルバージョンとの不一致を判定する通信管理テーブルバージョン判定部と、

上記通信管理テーブルバージョン判定部により不一致と判定された場合に、上記管理装置側通信管理テーブルを送信する通信管理テーブル送信部とを備え、

上記暗号装置は、更に、上記管理装置から上記管理装置側通信管理テーブルを受信する通信管理テーブル受信部を備え、

上記暗号装置側通信管理テーブル記憶部は、上記通信管理テーブル受信部により受信された上記管理装置側通信管理テーブルを、上記暗号装置側通信管理テーブルとして記憶することを特徴とする。

上記通信管理テーブル送信部は、上記通信管理テーブルバージョン判定部により不一致と判定された場合に、更に、上記管理装置側通信管理テーブルバージョンを送信し、

上記通信管理テーブル受信部は、更に、上記管理装置から上記管理装置側通信管理テーブルバージョンを受信し、

上記暗号装置側通信管理テーブルバージョン記憶部は、上記通信管理テーブル受信部により受信された上記管理装置側通信管理テーブルバー

ジョンを、上記暗号装置側通信管理テーブルバージョンとして記憶することを特徴とする。

この発明に係る管理装置は、インターネットを介して互いに接続する複数の暗号装置が通信に用いる通信管理テーブルを管理する管理装置であって、

上記管理装置で記憶する上記通信管理テーブルである管理装置側通信管理テーブルを記憶する管理装置側通信管理テーブル記憶部と、

上記管理装置側通信管理テーブルのバージョンである管理装置側通信管理テーブルバージョンを記憶する管理装置側通信管理テーブルバージョン記憶部と、

上記暗号装置から、上記暗号装置で記憶する上記通信管理テーブルである暗号装置側通信管理テーブルのバージョンである暗号装置側通信管理テーブルバージョンを受信する通信管理テーブルバージョン受信部と、

受信した上記暗号装置側通信管理テーブルバージョンと、上記管理装置側通信管理テーブルバージョンとの不一致を判定する通信管理テーブルバージョン判定部と、

上記通信管理テーブルバージョン判定部により不一致と判定された場合に、上記管理装置側通信管理テーブルを送信する通信管理テーブル送信部とを備えることを特徴とする。

上記通信管理テーブル送信部は、上記通信管理テーブルバージョン判定部により不一致と判定された場合に、更に、上記管理装置側通信管理テーブルバージョンを送信することを特徴とする。

上記管理装置は、更に、上記管理装置側通信管理テーブルと、上記管理装置側通信管理テーブルバージョンとを対応付けて更新する管理装置側通信管理テーブル更新部を有することを特徴とする。

上記管理装置は、更に、上記管理装置側通信管理テーブルの中で更新する情報である通信管理テーブル更新情報を受信する通信管理テーブル更新情報受信部を有することを特徴とする。

この発明に係る暗号装置は、インターネットを介して他の暗号装置と接続し、通信に用いる通信管理テーブルを管理装置によって管理される暗号装置であって、

上記暗号装置は、上記暗号装置で記憶する上記通信管理テーブルである暗号装置側通信管理テーブルを記憶する暗号装置側通信管理テーブル記憶部と、

上記暗号装置側通信管理テーブルのバージョンである暗号装置側通信管理テーブルバージョンを記憶する暗号装置側通信管理テーブルバージョン記憶部と、

上記暗号装置側通信管理テーブルバージョンを、上記管理装置へ送信する通信管理テーブルバージョン送信部と、

上記管理装置から、上記管理装置で記憶する上記通信管理テーブルである管理装置側通信管理テーブルを受信する通信管理テーブル受信部とを備え、

上記暗号装置側通信管理テーブル記憶部は、上記通信管理テーブル受信部により受信された上記管理装置側通信管理テーブルを、上記暗号装置側通信管理テーブルとして記憶することを特徴とする。

上記通信管理テーブル受信部は、更に、上記管理装置から上記管理装置側通信管理テーブルのバージョンである管理装置側通信管理テーブルバージョンを受信し、

上記暗号装置側通信管理テーブルバージョン記憶部は、上記通信管理テーブル受信部により受信された上記管理装置側通信管理テーブルバージョンを、上記暗号装置側通信管理テーブルバージョンとして記憶する

ことを特徴とする。

上記通信管理テーブルは、公開鍵を含み、

上記暗号装置は、更に、上記他の暗号装置と上記インターネットを介して秘匿通信を行なう際に用いる秘匿通信用秘密鍵を、上記暗号装置側通信管理テーブルに含まれる上記公開鍵を用いて上記他の暗号装置と共有化する秘匿鍵通信用秘密鍵交換部を備えることを特徴とする。

上記通信管理テーブルは、公開鍵を含み、

上記暗号装置は、更に、上記他の暗号装置と上記インターネットを介して秘匿通信を行なう際に用いる秘匿通信用認証鍵を、上記暗号装置側通信管理テーブルに含まれる上記公開鍵を用いて上記他の暗号装置と共有化する秘匿鍵通信用認証鍵交換部を備えることを特徴とする。

上記他の暗号装置は、サブネットに接続し、

上記通信管理テーブルは、上記サブネットの構成についての情報であるサブネット構成情報を含み、

上記暗号装置は、更に、上記暗号装置側通信管理テーブルに含まれる上記サブネット構成情報に基づいて、上記他の暗号装置と上記インターネットを介して通信を行なうインターネット通信部を有することを特徴とする。

この発明に係る通信管理テーブル転送方法は、インターネットを介して互いに接続し、それぞれ、暗号装置側通信管理テーブルを記憶する暗号装置側通信管理テーブル記憶部と、暗号装置側通信管理テーブルバージョンを記憶する暗号装置側通信管理テーブルバージョン記憶部とを有する複数の暗号装置と、

上記複数の暗号装置が通信に用いる通信管理テーブルを管理し、管理装置側通信管理テーブルを記憶する管理装置側通信管理テーブル記憶部と、管理装置側通信管理テーブルバージョンを記憶する管理装置側通信

管理テーブルバージョン記憶部とを有する管理装置とからなる通信管理テーブル転送システムの通信管理テーブル転送方法であって、

上記暗号装置が、上記暗号装置側通信管理テーブルバージョンを、上記管理装置へ送信する工程と、

上記管理装置が、上記暗号装置から上記暗号装置側通信管理テーブルバージョンを受信する工程と、

上記管理装置が、受信した上記暗号装置側通信管理テーブルバージョンと、上記管理装置側通信管理テーブルバージョンとの不一致を判定する工程と、

上記工程で不一致と判定した場合に、上記管理装置が、上記管理装置側通信管理テーブルを送信する工程と、

上記暗号装置が、上記管理装置から上記管理装置側通信管理テーブルを受信する工程と、

上記暗号装置が、受信した上記管理装置側通信管理テーブルを、上記暗号装置側通信管理テーブルとして記憶する工程とを有することを特徴とする。

図面の簡単な説明

図１は、本実施例における暗号装置の構成を示す図である。

図２は、本実施例における管理装置の構成を示す図である。

図３は、本実施例における電源を入れたときの通信管理テーブルの転送の手順を示す図である。

図４は、本実施例における電源を入れたときの通信管理テーブルの転送を省略する手順を示す図である。

図５は、本実施例におけるリブートされたときの通信管理テーブルの転送の手順を示す図である。

図６は、本実施例におけるリブートされたときの通信管理テーブルの転送を省略する手順を示す図である。

図７は、本実施例における通信管理テーブルの構成を示す図である。

図８は、本実施例における通信管理テーブルの構成を示す図である。

図９は、本実施例における通信管理テーブルの構成を示す図である。

図１０は、ＳＡ確立の際のデータフローを示す図である。

図１１は、秘匿通信の際のデータフローを示す図である。

図１２は、サブネット構成情報の使用例を示す図である。

図１３は、仮想私設網を用いるシステムの例を示す図である。

図１４は、従来例における電源を入れたときの通信管理テーブルの転送の手順を示す図である。

図１５は、従来例におけるリブートされたときの通信管理テーブルの転送の手順を示す図である。

発明を実施するための最良の形態

実施の形態１.

以下、本発明を図面に示す実施例に基づいて説明する。

図１は、本実施例における暗号装置の構成を示す図である。１００１は、電源制御部、１００２は、リブート制御部、１００３は、初期化部、１００４は、暗号装置側通信管理テーブル記憶部、１００５は、暗号装置側通信管理テーブルバージョン記憶部、１００６は、通信管理テーブルバージョン暗号化部、１００７は、初期化完了通知部、１００８は、通信管理テーブルダウンロード制御部、１００９は、通信管理テーブル受信部である。

図２は、本実施例における管理装置の構成を示す図である。２００１は、リブート指示部、２００２は、初期化完了受信部、２００３は、通

信管理テーブルバージョン復号部、２００４は、管理装置側通信管理テーブル記憶部、２００５は、管理装置側通信管理テーブルバージョン記憶部、２００６は、通信管理テーブルバージョン判定部、２００７は、通信管理テーブルダウンロード指示部、２００８は、通信管理テーブル送信部である。

図３は、本実施例おける電源を入れたときの通信管理テーブルの転送の手順を示す図である。以下、この手順について、図１及び図２の構成に基づいて説明する。

暗号装置Ａ１１側では、電源が入れられると、電源制御部１００１が初期化部１００３に初期化を指示する。初期化部１００３は、初期化を完了すると初期化完了通知部１００７に初期化の完了を知らせる。初期化完了通知部１００７は、管理装置３６の初期化完了受信部２００２に暗号装置初期化完了通知（Ｓ３０１）を送信する。このとき管理装置３６の公開鍵により暗号化した通信管理テーブルバージョンが、暗号装置初期化完了通知（Ｓ３０１）に含まれている。

通信管理テーブルバージョンは、暗号装置側通信管理テーブルバージョン記憶部１００５に記憶されている。暗号装置側通信管理テーブルバージョン記憶部１００５の通信管理テーブルバージョンは、暗号装置側通信管理テーブル記憶部１００４の通信管理テーブルと対応付けられている。この例では、暗号装置側通信管理テーブルバージョン記憶部１００５は、暗号装置側通信管理テーブル記憶部１００４に含まれるが、別個に設けても構わない。

通信管理テーブルバージョン暗号化部１００６は、暗号装置側通信管理テーブルバージョン記憶部１００５から通信管理テーブルバージョンを読み、これを暗号化し、暗号化された通信管理テーブルバージョンを初期化完了通知部１００７に送るように構成されている。

管理装置３６側では、初期化完了受信部２００２が、暗号装置初期化完了通知（Ｓ３０１）を受信し、通信管理テーブルバージョン復号部２００３が、暗号化されている通信管理テーブルバージョンを復号する。一方、通信管理テーブルバージョン判定部２００６は、管理装置側通信管理テーブルバージョン記憶部２００５から管理装置３６側で記憶する通信管理テーブルバージョンを読む。そして、通信管理テーブルバージョン判定部２００６は、これらの通信管理テーブルバージョンを比較する。尚、この実施例では、管理装置側通信管理テーブルバージョン記憶部２００５は、管理装置側通信管理テーブル記憶部２００４に含められているが、通信管理テーブルと通信管理テーブルバージョンが対応付けられていれば、別個に設けても構わない。

比較の結果、２つの通信管理テーブルバージョンが不一致の場合には、通信管理テーブルバージョン判定部２００６は、通信管理テーブルダウンロード指示部２００７に不一致を知らせる。

通信管理テーブルダウンロード指示部２００７は、不一致の知らせを受けると、暗号装置Ａ１１の通信管理テーブルダウンロード制御部１００８に通信管理テーブルダウンロード指示（Ｓ３０２）を送信する。

暗号装置Ａ１１側では、通信管理テーブルダウンロード制御部１００８が、通信管理テーブルダウンロード指示（Ｓ３０２）を受信するとファイル転送の手順に従って通信管理テーブルを受信する為に、通信管理テーブル受信部１００９に通信管理テーブル取得の指示を送る。

通信管理テーブル受信部１００９は、その指示を受けると、管理装置３６の通信管理テーブル送信部２００８に通信管理テーブル取得命令（Ｓ１０３）を送る。

管理装置３６側では、通信管理テーブル取得命令（Ｓ１０３）を受けた通信管理テーブル送信部２００８は、管理装置側通信管理テーブル記

憶部２００４から通信管理テーブルを読み、その通信管理テーブルを暗号装置Ａ１１の通信管理テーブル受信部１００９にファイル転送する（Ｓ１０４）。

暗号装置Ａ１１側では、通信管理テーブル受信部１００９が通信管理テーブルを受信し終えると、通信管理テーブルダウンロード制御部１００８に通信管理テーブル取得の完了を知らせ、通信管理テーブルダウンロード制御部１００８は通信管理テーブルダウンロード指示応答（Ｓ１０５）を管理装置３６の通信管理テーブルダウンロード指示部２００７に送信する。また、通信管理テーブル受信部１００９は、受信した通信管理テーブルを暗号装置側通信管理テーブル記憶部１００４に記憶する。

この例では、ファイル転送のときに通信管理テーブルに通信管理テーブルバージョンを含めて転送し、暗号装置側通信管理テーブル記憶部１００４は通信管理テーブルバージョンを含む通信管理テーブル記憶している。しかし、通信管理テーブルバージョンを、通信管理テーブルに含めない構成にすることもできる。つまり、通信管理テーブルバージョンを含まない通信管理テーブルと、通信管理テーブルバージョンを別個にファイル転送することも可能である。

このようにして、通信管理テーブルバージョンが一致しない場合は、通信管理テーブルが管理装置３６から暗号装置Ａ１１へ転送される。また、通信管理テーブルバージョンも転送される。

図４は、本実施例における電源を入れたときの通信管理テーブルの転送を省略する手順を示す図である。以下、この手順について、図１及び図２の構成に基づいて説明する。

通信管理テーブルバージョン判定部２００６が、通信管理テーブルバージョンを比較するまでの手順は、上述の手順と同様である。

比較の結果、通信管理テーブルバージョンが一致した場合には、通信管理テーブルバージョン判定部２００６は、一致を初期化完了受信部２００２に知らせる。

初期化完了受信部２００２は、暗号装置初期化完了通知応答（Ｓ１０２）を初期化完了通知部１００７に送信する。初期化完了通知部１００７が、暗号装置初期化完了通知応答（Ｓ１０２）を受け取ると動作を終了する。つまり、通信管理テーブルバージョンが一致する場合は、通信管理テーブルの転送は行なわれない。

暗号装置Ａ１１が通信管理テーブルバージョンを送信し、管理装置３６が通信管理テーブルバージョンを判定するタイミングは、初期化の時に限られない。システムで自由に設定することができる。例えば、リブートのタイミングや、定期的なタイミングであっても構わない。

図５は、本実施におけるリブートされたときの通信管理テーブルの転送の手順を示す図である。また、図６は、本実施におけるリブートされたときの通信管理テーブルの転送を省略する手順を示す図である。リブート指示（Ｓ２０１）とリブート指示応答（Ｓ２０２）に基づく再起動から始まる点を除き、図３及び図４の手順と同様である。

次に、通信管理テーブルの構成について説明する。図７、図８及び図９は本実施例における通信管理テーブルの構成を示す図である。

通信管理テーブルには、通信管理テーブルバージョン９０のほか、インターネット通信用情報Ａ５０、インターネット通信用情報Ｂ６０等のインターネット通信用情報と、サブネット構成情報Ａ７０、サブネット構成情報Ｂ８０等のサブネット構成情報が含まれる。

インターネット通信用情報Ａ５０は、暗号装置Ａ１１がインターネット１を介して、他の暗号装置と通信する場合に必要になる情報である。インターネット通信用情報Ｂ６０も同様に、暗号装置Ｂ２１がインター

ネット１を介して、他の暗号装置と通信する場合に必要になる情報である。

５１、６１は、インターネットアドレス、５２、６２は、暗号装置の識別子、５３、６３は、認証書、５４、６４は有効期限である。認証書には、ＳＡ用公開鍵が含まれている。

サブネット構成情報Ａ７０は、サブネット１４の構成に関する情報である。この図では、１レコードのみ示しているが、サブネット１４の構成に含まれる通信端末が多い場合には、更にレコードが付加されている。サブネット構成情報Ｂ８０も同様である。

７１、８１は、暗号装置の識別子、７２、８２は、ネットワークアドレス、７３、８３は、ネットマスクである。

図７の例では、通信管理テーブルバージョン９０は、バージョンは一つであり、通信管理テーブル全体の更新状況に対応している。

図８の例では、通信管理テーブルバージョン９０は、暗号装置Ａ情報バージョン９１、暗号装置Ｂ情報バージョン９２等複数のバージョンから構成されている。暗号装置Ａ情報バージョン９１は、インターネット通信用情報Ａ５０とサブネット構成情報Ａ７０等（サブネット構成情報Ａ７０の他にサブネット構成情報がある場合にはそれらも含む。）の更新状況に対応している。

図９の例では、更に細分化し、通信管理テーブルバージョン９０は、暗号装置Ａインターネット通信用情報バージョン９３、暗号装置Ａサブネット構成情報バージョン９４、暗号装置Ｂインターネット通信用情報バージョン９５、暗号装置Ｂサブネット構成情報バージョン９６等のバージョンから構成されている。暗号装置Ａインターネット通信用情報バージョン９３は、インターネット通信用情報Ａ５０の更新状況に対応している。また、暗号装置Ａサブネット構成情報バージョン９４は、サブ

ネット構成情報Ａ７０等（サブネット構成情報Ａ７０の他にサブネット構成情報がある場合にはそれらも含む。）の更新状況に対応している。

図８と図９の場合に、バージョンと各情報との対応をつけるために、各バージョンに対応して装置識別子や情報識別子を記憶する方法も考えられる。

管理装置３６は、各暗号装置から、通信管理テーブルの中で更新する情報である通信管理テーブル更新情報を受信する通信管理テーブル更新情報受信部（図示せず）と、管理装置側通信管理テーブルと、管理装置側通信管理テーブルバージョンとを対応付けて更新する管理装置側通信管理テーブル更新部（図示せず）を有する。

図７の場合、通信管理テーブル更新情報受信部は、いずれの暗号装置から通信管理テーブル更新情報を受信した場合にも、通信管理テーブルバージョン９０を更新する。図８の場合、通信管理テーブル更新情報受信部は、暗号装置Ａ１１から通信管理テーブル更新情報を受信した場合には、インターネット通信用情報Ａ５０、サブネット構成情報Ａ７０のいずれか若しくは両方を更新し、更に暗号装置Ａ情報バージョン９１を更新する。図９の場合、通信管理テーブル更新情報受信部は、暗号装置Ａ１１から通信管理テーブル更新情報を受信した場合には、インターネット通信用情報Ａ５０に関する通信管理テーブル更新情報、サブネット構成情報Ａ７０に関する通信管理テーブル更新情報のいずれか若しくは両方かを判断し、その部分を更新し、更にその部分に対応する暗号装置Ａインターネット通信用情報バージョン９３、暗号装置Ａサブネット構成情報バージョン９４のいずれか若しくは両方を更新する。

図８や図９のように、通信管理テーブルバージョンを細分化した場合には、通信管理テーブルバージョン判定部２００６は、細分化したバージョン毎に比較し、通信管理テーブルのうち不一致のバージョンに関す

る部分のみを通信管理テーブル転送（Ｓ１０４）で転送するようにすることも有効である。その場合は、通信管理テーブルダウンロード指示（Ｓ３０２）に転送する部分を特定する情報を付加し、通信管理テーブル受信部１００９は、暗号装置側通信管理テーブル記憶部１００４の中のその部分のみを更新し、暗号装置側通信管理テーブルバージョン記憶部１００５の中のその部分のバージョンのみを更新する。

次に、通信管理テーブルに含まれるＳＡ用公開鍵を用いてＳＡを確立する動作について説明する。図１０は、ＳＡ確立の際のデータフローを示す図である。この例では、暗号装置Ａ１１がＳＡ確立を要求する側であり、暗号装置Ｂ２１がＳＡ確立の要求に応答する側である。それぞれの暗号装置は、自らのＳＡ用秘密鍵を記憶するＳＡ用秘密鍵記憶部１０１３と、秘匿通信用秘密鍵１０１１と秘匿通信用認証鍵１０１２を共有化する秘匿通信用認証鍵秘密鍵交換部１０１０とを有する。秘匿通信用認証鍵秘密鍵交換部１０１０は、図に示すように、自らのＳＡ用秘密鍵と、相手側のＳＡ用公開鍵とを入力できるように構成されている。

暗号装置Ａ１１の秘匿通信用認証鍵秘密鍵交換部１０１０は、乱数Ｘａを生成し、署名し、暗号化し、暗号装置Ｂ２１側へ送信する（Ｓ５０１）。暗号装置Ｂ２１の秘匿通信用認証鍵秘密鍵交換部１０１０は、乱数Ｘｂを生成し、乱数Ｘａと組合わせて秘匿通信用秘密鍵１０１１と秘匿通信用認証鍵１０１２を生成する。更に、ＸｂとＸａのハッシュ値を署名し、暗号化し、暗号装置Ａ１１側へ送信する（Ｓ５０２）。暗号装置Ａ１１の秘匿通信用認証鍵秘密鍵交換部１０１０は、乱数Ｘａと乱数Ｘｂとを組合わせて秘匿通信用秘密鍵１０１１と秘匿通信用認証鍵１０１２を生成し、受信したハッシュ値を検証する。更に乱数Ｘｂのハッシュ値を暗号装置Ｂ２１側に送信する（Ｓ５０３）。暗号装置Ｂ２１の秘匿通信用認証鍵秘密鍵交換部１０１０は、受信したハッシュ値を検証す

る。以上の手順により、ＳＡが確立する。これによって、両者は、共通の秘匿通信用秘密鍵１０１１と秘匿通信用認証鍵１０１２を取得する。

次に、ＳＡ確立の後に行われる秘匿通信の動作について説明する。図１１は、秘匿通信の際のデータフローを示す図である。この例では、暗号装置Ａ１１がデータを送信する側であり、暗号装置Ｂ２１がデータを受信する側である。但し、ＳＡが確立している暗号装置間では、双方向の通信が可能であり、この例に限定されない。

それぞれの暗号装置は、インターネット通信部１０１４と、サブネット通信部１０１５とを有する。インターネット通信部１０１４は、インターネット１を介する通信を制御し、サブネット通信部１０１５は、サブネットを介する通信を制御する。

送信側のインターネット通信部１０１４は、暗号化部１０１６と、認証部１０１７と、エンカプセル処理部１０１８が動作する。また、受信側のインターネット通信部１０１４は、認証部１０１９と、復号部１０２０と、デカプセル処理部１０２１が動作する。この動作において、秘匿通信用秘密鍵１０１１は、暗号アルゴリズムに使用され、秘匿通信用認証鍵１０１２は、認証アルゴリズムに使用される。

また、通信管理テーブルに含まれるサブネット構成情報は、他の暗号装置に接続されるサブネットに対して通信を行なう場合に用いられる。図１２に示すように、サブネット構成情報は、インターネット通信部１０１４で用いられる。

産業上の利用可能性

本発明においては、管理装置と暗号装置の間で、通信管理テーブルのバージョンを管理し、両者間の通信管理テーブルの同一性が確認できた場合には、通信管理テーブルの転送を行なわないように構成したので、

通信管理テーブルの転送回数が削減され、データ通信の性能及び安全性が著しく向上する。

請求の範囲

1．インターネットを介して互いに接続する複数の暗号装置と、上記複数の暗号装置が通信に用いる通信管理テーブルを管理する管理装置とからなる通信管理テーブル転送システムであって、

上記暗号装置は、上記暗号装置で記憶する上記通信管理テーブルである暗号装置側通信管理テーブルを記憶する暗号装置側通信管理テーブル記憶部と、

上記暗号装置側通信管理テーブルのバージョンである暗号装置側通信管理テーブルバージョンを記憶する暗号装置側通信管理テーブルバージョン記憶部と、

上記暗号装置側通信管理テーブルバージョンを、上記管理装置へ送信する通信管理テーブルバージョン送信部とを備え、

上記管理装置は、上記管理装置で記憶する上記通信管理テーブルである管理装置側通信管理テーブルを記憶する管理装置側通信管理テーブル記憶部と、

上記管理装置側通信管理テーブルのバージョンである管理装置側通信管理テーブルバージョンを記憶する管理装置側通信管理テーブルバージョン記憶部と、

上記暗号装置から上記暗号装置側通信管理テーブルバージョンを受信する通信管理テーブルバージョン受信部と、

受信した上記暗号装置側通信管理テーブルバージョンと、上記管理装置側通信管理テーブルバージョンとの不一致を判定する通信管理テーブルバージョン判定部と、

上記通信管理テーブルバージョン判定部により不一致と判定された場合に、上記管理装置側通信管理テーブルを送信する通信管理テーブル送

信部とを備え、

上記暗号装置は、更に、上記管理装置から上記管理装置側通信管理テーブルを受信する通信管理テーブル受信部を備え、

上記暗号装置側通信管理テーブル記憶部は、上記通信管理テーブル受信部により受信された上記管理装置側通信管理テーブルを、上記暗号装置側通信管理テーブルとして記憶することを特徴とする通信管理テーブル転送システム。

2．上記通信管理テーブル送信部は、上記通信管理テーブルバージョン判定部により不一致と判定された場合に、更に、上記管理装置側通信管理テーブルバージョンを送信し、

上記通信管理テーブル受信部は、更に、上記管理装置から上記管理装置側通信管理テーブルバージョンを受信し、

上記暗号装置側通信管理テーブルバージョン記憶部は、上記通信管理テーブル受信部により受信された上記管理装置側通信管理テーブルバージョンを、上記暗号装置側通信管理テーブルバージョンとして記憶することを特徴とする請求項１記載の通信管理テーブル転送システム。

3．インターネットを介して互いに接続する複数の暗号装置が通信に用いる通信管理テーブルを管理する管理装置であって、

上記管理装置で記憶する上記通信管理テーブルである管理装置側通信管理テーブルを記憶する管理装置側通信管理テーブル記憶部と、

上記管理装置側通信管理テーブルのバージョンである管理装置側通信管理テーブルバージョンを記憶する管理装置側通信管理テーブルバージョン記憶部と、

上記暗号装置から、上記暗号装置で記憶する上記通信管理テーブルである暗号装置側通信管理テーブルのバージョンである暗号装置側通信管理テーブルバージョンを受信する通信管理テーブルバージョン受信部と

受信した上記暗号装置側通信管理テーブルバージョンと、上記管理装置側通信管理テーブルバージョンとの不一致を判定する通信管理テーブルバージョン判定部と、

上記通信管理テーブルバージョン判定部により不一致と判定された場合に、上記管理装置側通信管理テーブルを送信する通信管理テーブル送信部とを備えることを特徴とする管理装置。

4．上記通信管理テーブル送信部は、上記通信管理テーブルバージョン判定部により不一致と判定された場合に、更に、上記管理装置側通信管理テーブルバージョンを送信することを特徴とする請求項3記載の管理装置。

5．上記管理装置は、更に、上記管理装置側通信管理テーブルと、上記管理装置側通信管理テーブルバージョンとを対応付けて更新する管理装置側通信管理テーブル更新部を有することを特徴とする請求項3記載の管理装置。

6．上記管理装置は、更に、上記管理装置側通信管理テーブルの中で更新する情報である通信管理テーブル更新情報を受信する通信管理テーブル更新情報受信部を有することを特徴とする請求項5記載の管理装置。

7．インターネットを介して他の暗号装置と接続し、通信に用いる通信管理テーブルを管理装置によって管理される暗号装置であって、

上記暗号装置は、上記暗号装置で記憶する上記通信管理テーブルである暗号装置側通信管理テーブルを記憶する暗号装置側通信管理テーブル記憶部と、

上記暗号装置側通信管理テーブルのバージョンである暗号装置側通信

管理テーブルバージョンを記憶する暗号装置側通信管理テーブルバージョン記憶部と、

上記暗号装置側通信管理テーブルバージョンを、上記管理装置へ送信する通信管理テーブルバージョン送信部と、

上記管理装置から、上記管理装置で記憶する上記通信管理テーブルである管理装置側通信管理テーブルを受信する通信管理テーブル受信部とを備え、

上記暗号装置側通信管理テーブル記憶部は、上記通信管理テーブル受信部により受信された上記管理装置側通信管理テーブルを、上記暗号装置側通信管理テーブルとして記憶することを特徴とする暗号装置。

8．上記通信管理テーブル受信部は、更に、上記管理装置から上記管理装置側通信管理テーブルのバージョンである管理装置側通信管理テーブルバージョンを受信し、

上記暗号装置側通信管理テーブルバージョン記憶部は、上記通信管理テーブル受信部により受信された上記管理装置側通信管理テーブルバージョンを、上記暗号装置側通信管理テーブルバージョンとして記憶することを特徴とする請求項7記載の暗号装置。

9．上記通信管理テーブルは、公開鍵を含み、

上記暗号装置は、更に、上記他の暗号装置と上記インターネットを介して秘匿通信を行なう際に用いる秘匿通信用秘密鍵を、上記暗号装置側通信管理テーブルに含まれる上記公開鍵を用いて上記他の暗号装置と共有化する秘匿鍵通信用秘密鍵交換部を備えることを特徴とする請求項7記載の暗号装置。

１０．上記通信管理テーブルは、公開鍵を含み、

上記暗号装置は、更に、上記他の暗号装置と上記インターネットを介して秘匿通信を行なう際に用いる秘匿通信用認証鍵を、上記暗号装置側

通信管理テーブルに含まれる上記公開鍵を用いて上記他の暗号装置と共有化する秘匿鍵通信用認証鍵交換部を備えることを特徴とする請求項７記載の暗号装置。

１１．上記他の暗号装置は、サブネットに接続し、

上記通信管理テーブルは、上記サブネットの構成についての情報であるサブネット構成情報を含み、

上記暗号装置は、更に、上記暗号装置側通信管理テーブルに含まれる上記サブネット構成情報に基づいて、上記他の暗号装置と上記インターネットを介して通信を行なうインターネット通信部を有することを特徴とする請求項７記載の暗号装置。

１２．インターネットを介して互いに接続し、それぞれ、暗号装置側通信管理テーブルを記憶する暗号装置側通信管理テーブル記憶部と、暗号装置側通信管理テーブルバージョンを記憶する暗号装置側通信管理テーブルバージョン記憶部とを有する複数の暗号装置と、

上記複数の暗号装置が通信に用いる通信管理テーブルを管理し、管理装置側通信管理テーブルを記憶する管理装置側通信管理テーブル記憶部と、管理装置側通信管理テーブルバージョンを記憶する管理装置側通信管理テーブルバージョン記憶部とを有する管理装置とからなる通信管理テーブル転送システムの通信管理テーブル転送方法であって、

上記暗号装置が、上記暗号装置側通信管理テーブルバージョンを、上記管理装置へ送信する工程と、

上記管理装置が、上記暗号装置から上記暗号装置側通信管理テーブルバージョンを受信する工程と、

上記管理装置が、受信した上記暗号装置側通信管理テーブルバージョンと、上記管理装置側通信管理テーブルバージョンとの不一致を判定する工程と、

上記工程で不一致と判定した場合に、上記管理装置が、上記管理装置側通信管理テーブルを送信する工程と、

上記暗号装置が、上記管理装置から上記管理装置側通信管理テーブルを受信する工程と、

上記暗号装置が、受信した上記管理装置側通信管理テーブルを、上記暗号装置側通信管理テーブルとして記憶する工程とを有することを特徴とする通信管理テーブル転送方法。

図 1

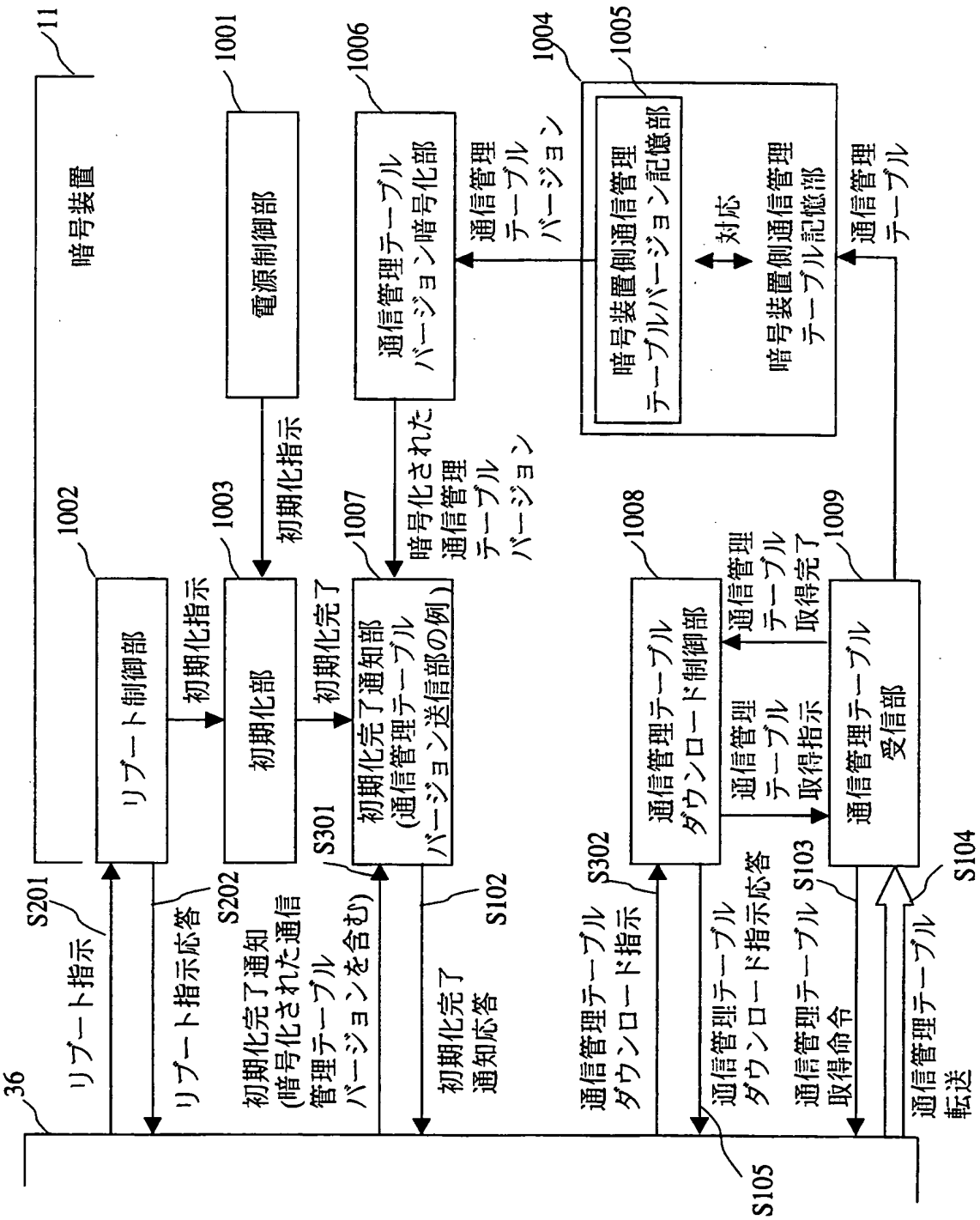

11
暗号装置
1001
電源制御部
1006
通信管理テーブル
バージョン暗号化部
1004
1005
暗号装置側通信管理
テーブルバージョン記憶部
対応
暗号装置側通信管理
テーブル記憶部
通信管理
テーブル
バージョン
1002
リブート制御部
初期化指示
1003
初期化部
初期化指示
1007
初期化完了通知部
(通信管理テーブル
バージョン送信部の例)
暗号化された
通信管理
テーブル
バージョン
1008
通信管理テーブル
ダウンロード制御部
通信管理
テーブル
取得指示
1009
通信管理テーブル
受信部
通信管理
テーブル
取得完了
36
リブート指示
S201
リブート指示応答
S202
初期化完了通知
(暗号化された通信
管理テーブル
バージョンを含む)
S301
初期化完了
通知応答
S102
通信管理テーブル
ダウンロード指示
S302
通信管理テーブル
ダウンロード指示応答
S103
通信管理テーブル
取得命令
S104
通信管理テーブル
転送
S105

図 2

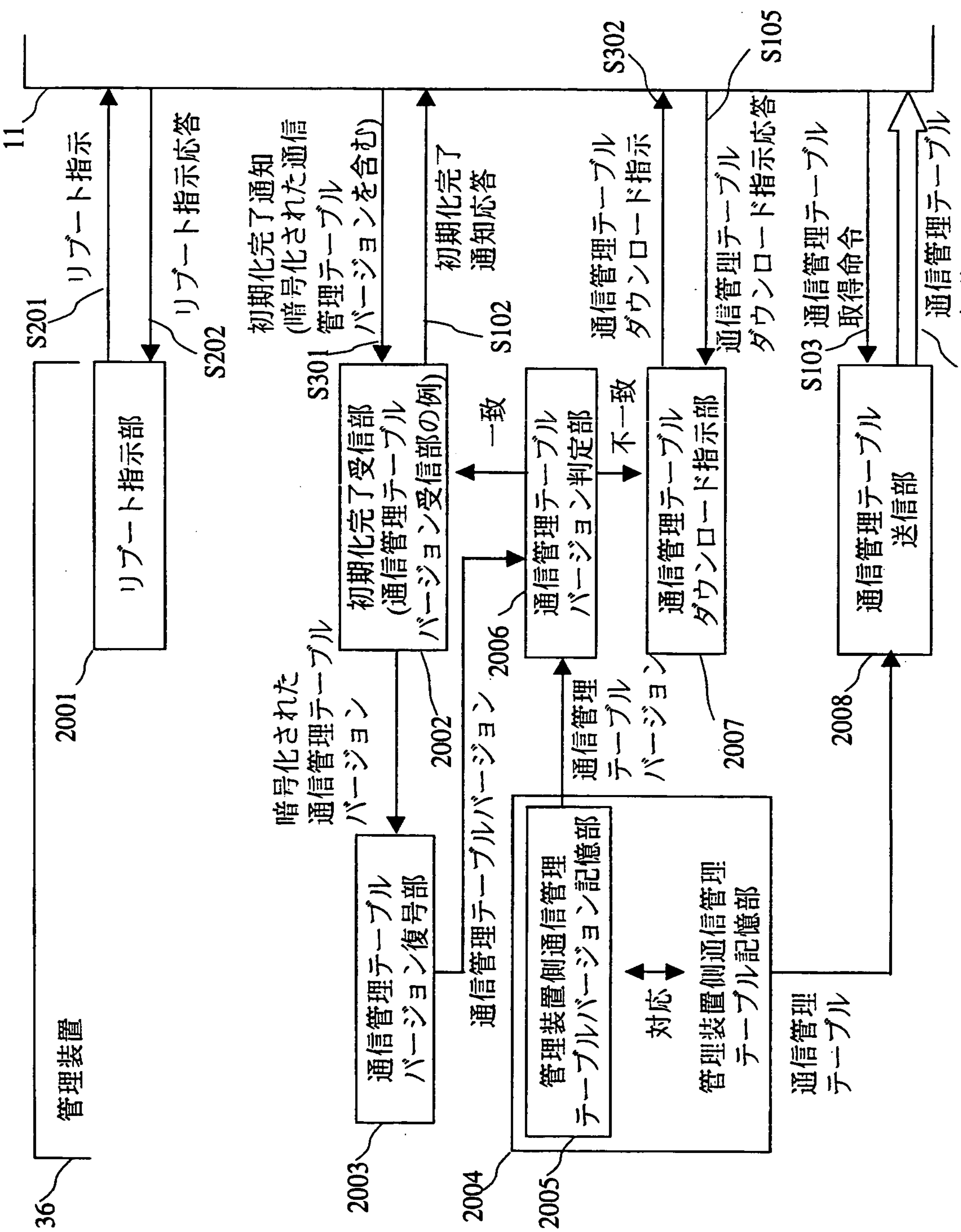

11
36
管理装置
2001
リブート指示部
S201
リブート指示
S202
リブート指示応答
2002
初期化完了受信部
(通信管理テーブル
バージョン受信部の例)
S301
初期化完了通知
(暗号化された通信
管理テーブル
バージョンを含む)
S102
初期化完了
通知応答
暗号化された
通信管理テーブル
バージョン
2003
通信管理テーブル
バージョン復号部
通信管理テーブルバージョン
2006
通信管理テーブル
バージョン判定部
一致
不一致
通信管理
テーブル
バージョン
2007
通信管理テーブル
ダウンロード指示部
S302
通信管理テーブル
ダウンロード指示
S105
通信管理テーブル
ダウンロード指示応答
2004
管理装置側通信管理
テーブル記憶部
2005
管理装置側通信管理
テーブルバージョン記憶部
対応
2008
通信管理テーブル
送信部
S103
通信管理テーブル
取得命令
S104
通信管理テーブル
転送
通信管理
テーブル

図 3

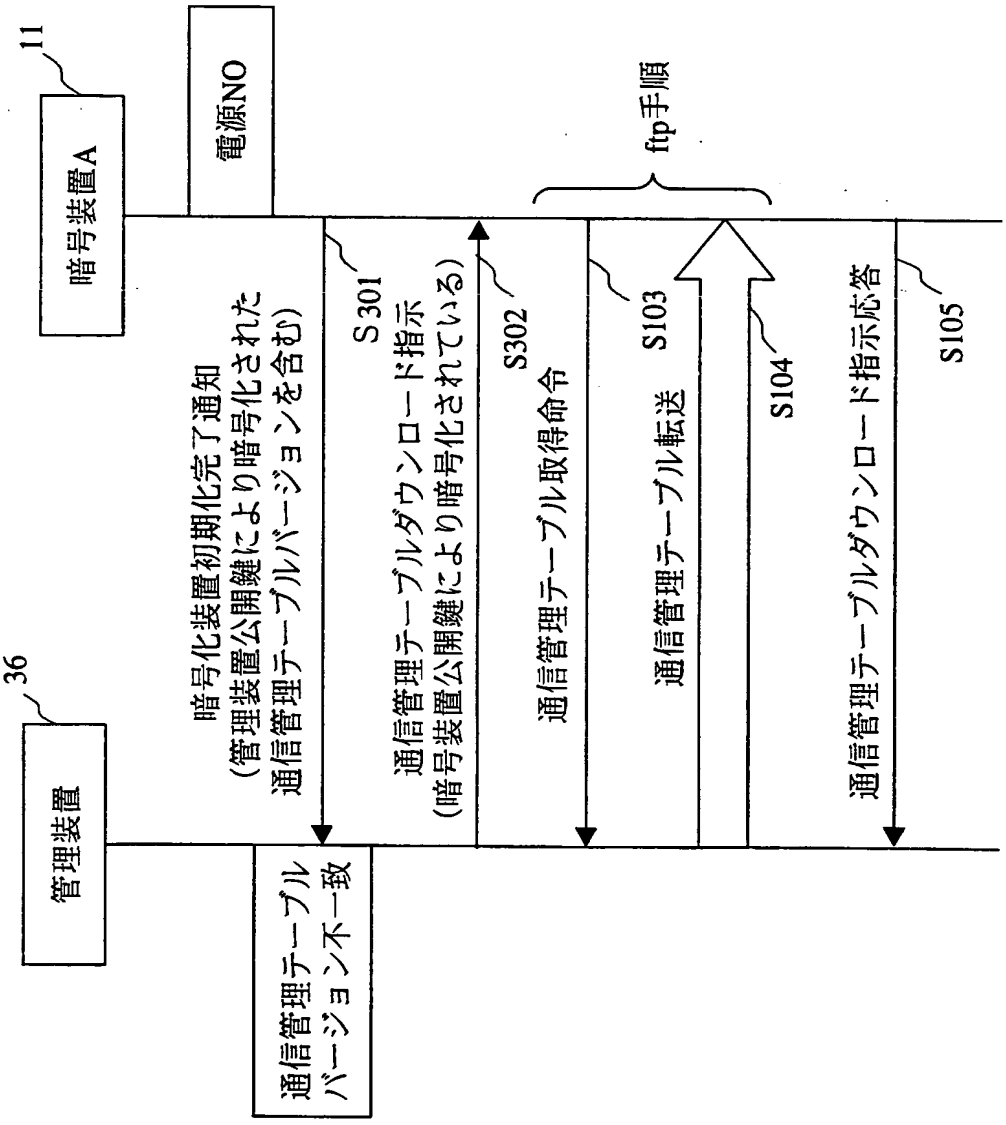
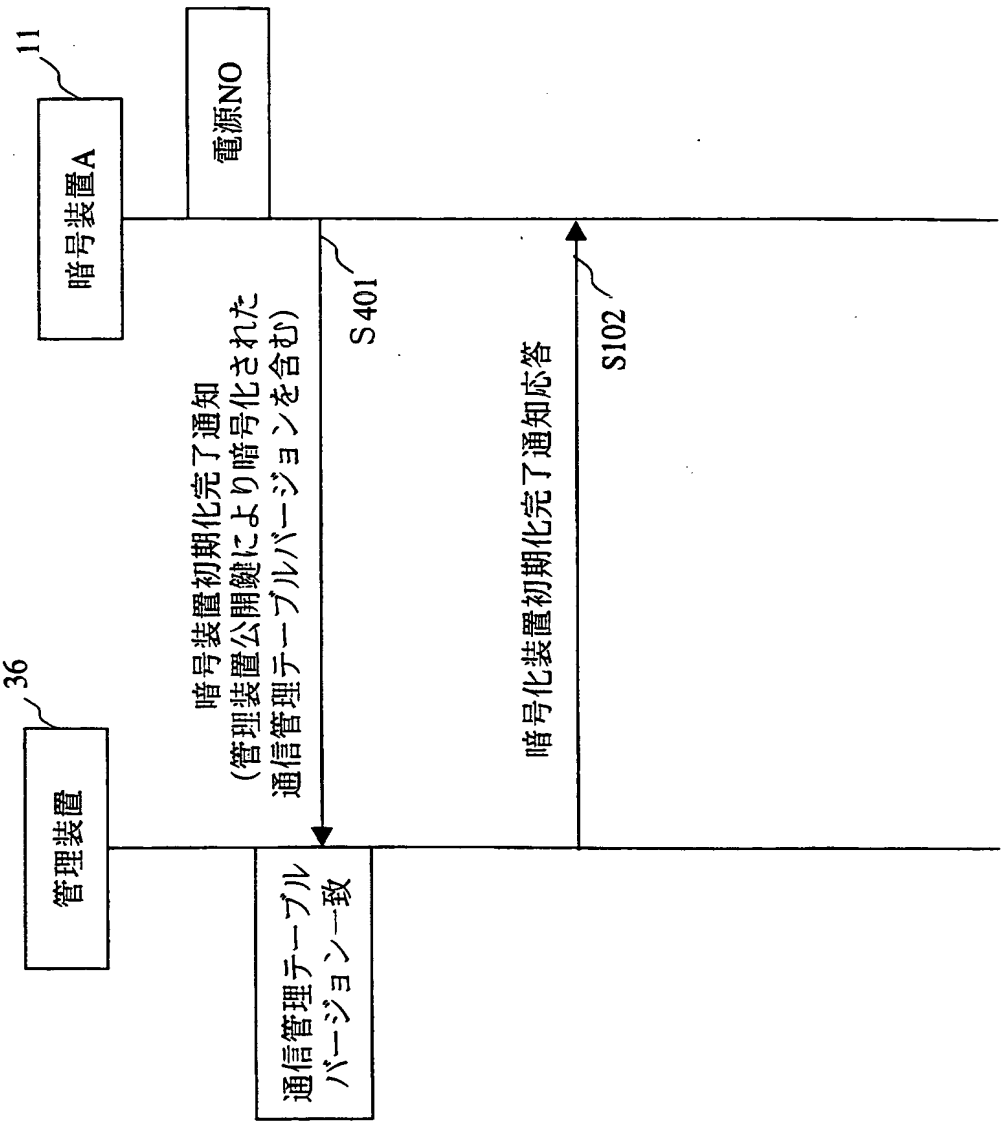

11
暗号装置A
電源NO
ftp手順
暗号化装置初期化完了通知
(管理装置公開鍵により暗号化された
通信管理テーブルバージョンを含む)
S301
通信管理テーブルダウンロード指示
(暗号装置公開鍵により暗号化されている)
S302
通信管理テーブル取得命令
S103
通信管理テーブル転送
S104
通信管理テーブルダウンロード指示応答
S105
36
管理装置
通信管理テーブル
バージョン不一致

図 4


11
暗号装置A
電源NO
暗号装置初期化完了通知
(管理装置公開鍵により暗号化された
通信管理テーブルバージョンを含む)
S401
暗号化装置初期化完了通知応答
S102
36
管理装置
通信管理テーブル
バージョン一致

5/15

図 5

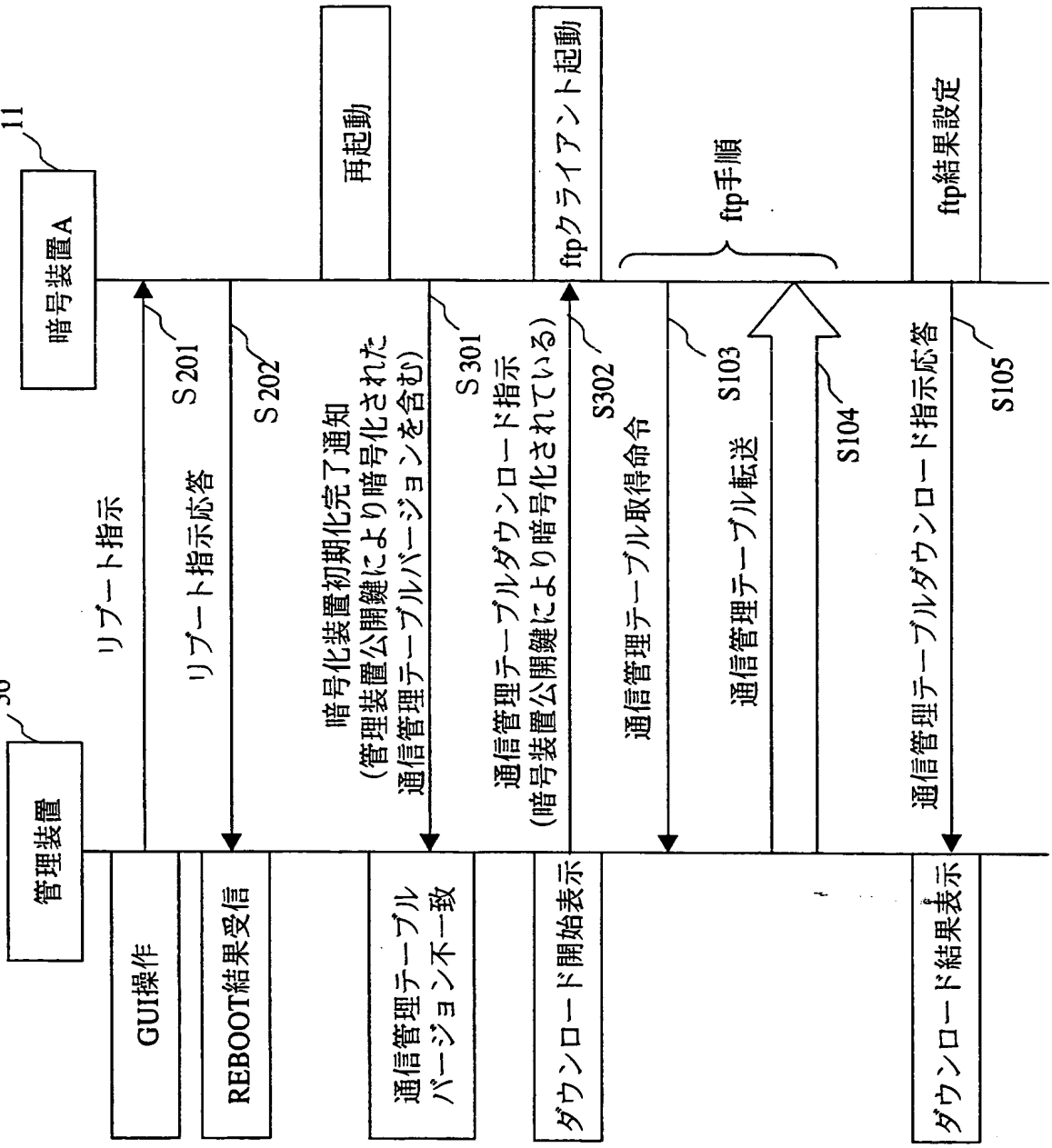

管理装置
36
暗号装置A
11
GUI操作
REBOOT結果受信
通信管理テーブル
バージョン不一致
ダウンロード開始表示
ダウンロード結果表示
リブート指示
リブート指示応答
S201
S202
暗号化装置初期化完了通知
(管理装置公開鍵により暗号化された
通信管理テーブルバージョンを含む)
再起動
S301
通信管理テーブルダウンロード指示
(暗号装置公開鍵により暗号化されている)
ftpクライアント起動
S302
通信管理テーブル取得命令
ftp手順
S103
通信管理テーブル転送
S104
通信管理テーブルダウンロード指示応答
S105
ftp結果設定

図 6

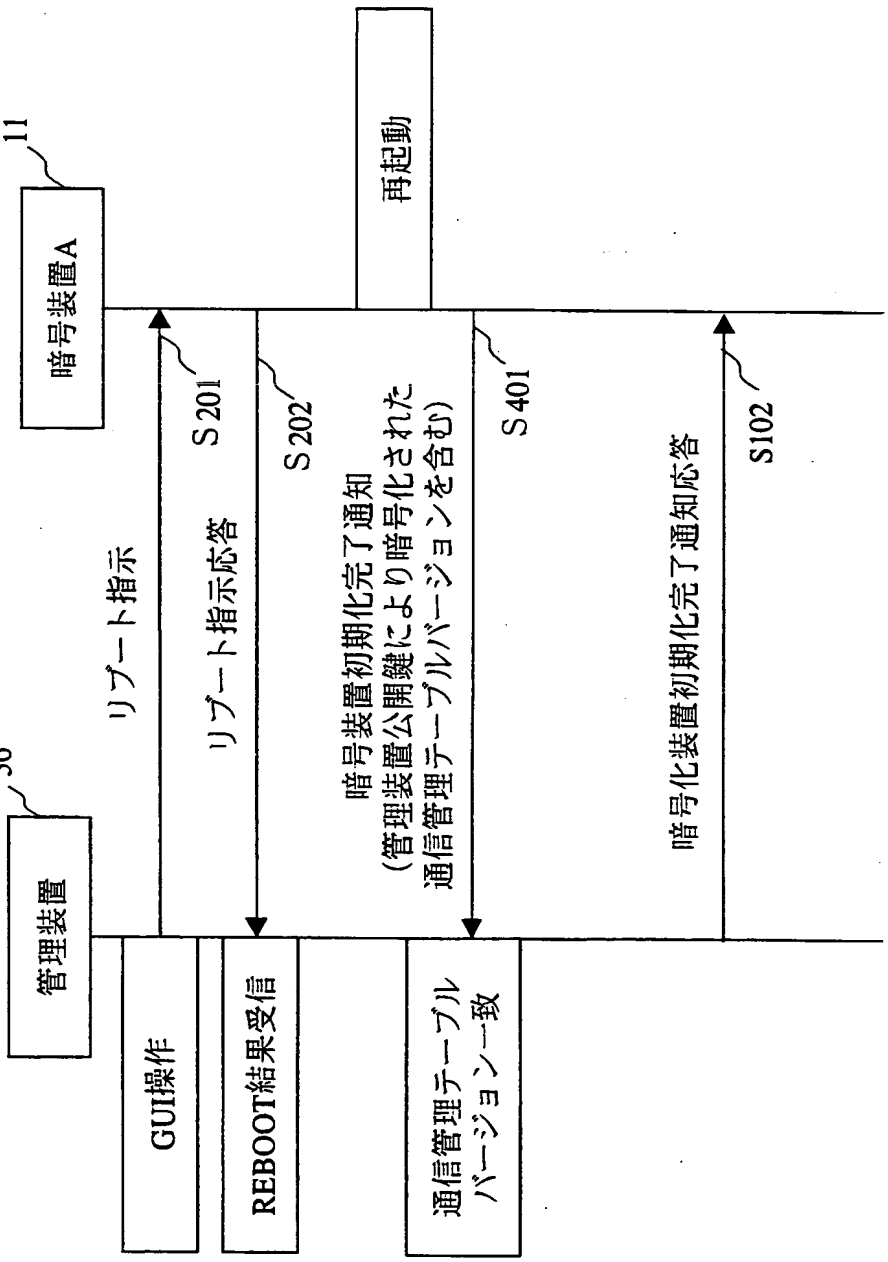

11
暗号装置A
再起動
36
管理装置
リブート指示
S201
リブート指示応答
S202
暗号装置初期化完了通知
(管理装置公開鍵により暗号化された
通信管理テーブルバージョンを含む)
S401
暗号化装置初期化完了通知応答
S102
GUI操作
REBOOT結果受信
通信管理テーブル
バージョン一致

図 7

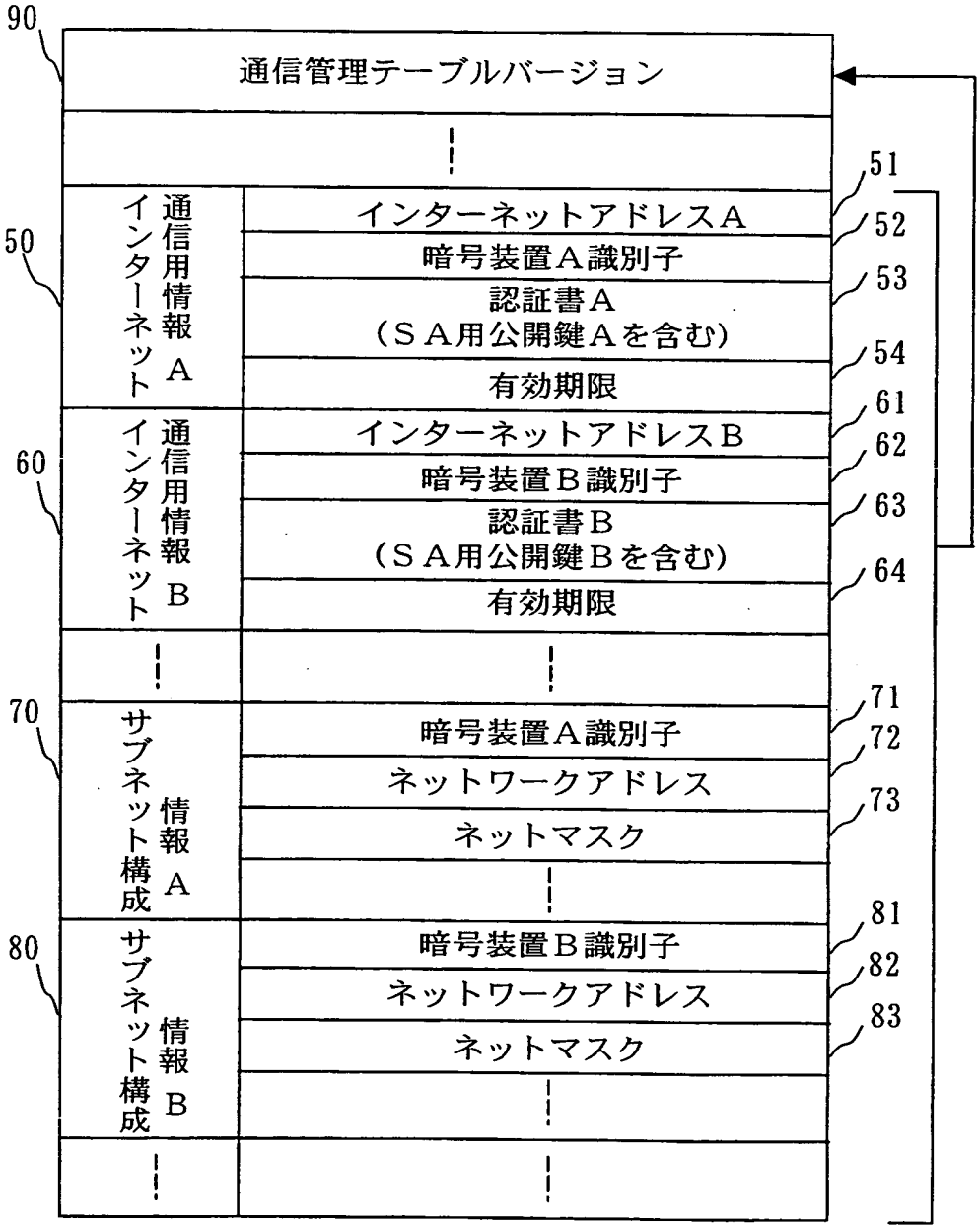

90
通信管理テーブルバージョン
50
通信用情報 インターネット A
インターネットアドレスA
51
暗号装置A識別子
52
認証書A
（SA用公開鍵Aを含む）
53
有効期限
54
60
通信用情報 インターネット B
インターネットアドレスB
61
暗号装置B識別子
62
認証書B
（SA用公開鍵Bを含む）
63
有効期限
64
70
サブネット構成 情報 A
暗号装置A識別子
71
ネットワークアドレス
72
ネットマスク
73
80
サブネット構成 情報 B
暗号装置B識別子
81
ネットワークアドレス
82
ネットマスク
83

図 8

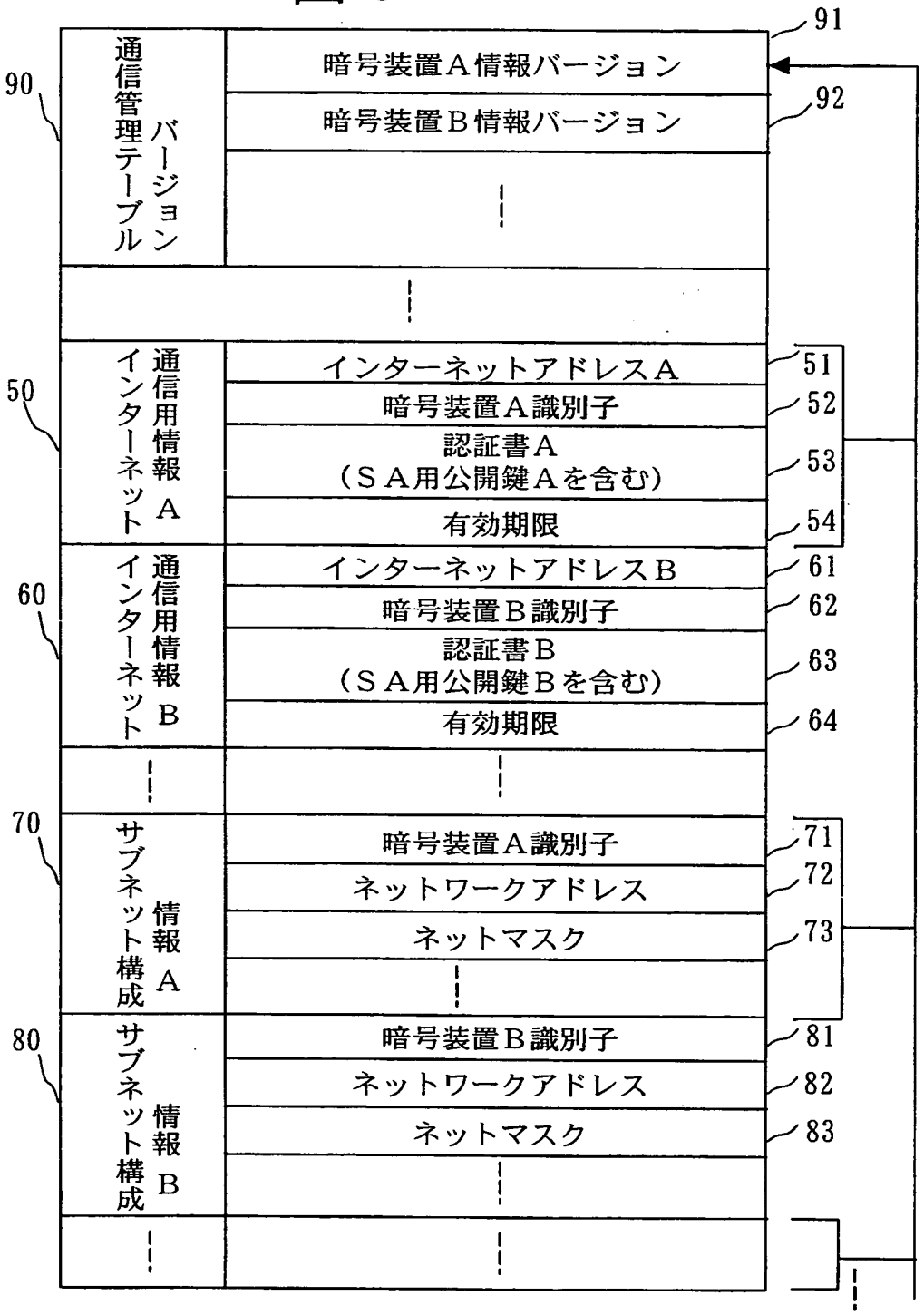

90
通信管理テーブル
バージョン
暗号装置A情報バージョン
暗号装置B情報バージョン
91
92
50
通信用情報 A
インターネット
インターネットアドレスA
暗号装置A識別子
認証書A
（SA用公開鍵Aを含む）
有効期限
51
52
53
54
60
通信用情報 B
インターネット
インターネットアドレスB
暗号装置B識別子
認証書B
（SA用公開鍵Bを含む）
有効期限
61
62
63
64
70
サブネット構成
情報 A
暗号装置A識別子
ネットワークアドレス
ネットマスク
71
72
73
80
サブネット構成
情報 B
暗号装置B識別子
ネットワークアドレス
ネットマスク
81
82
83

図 9

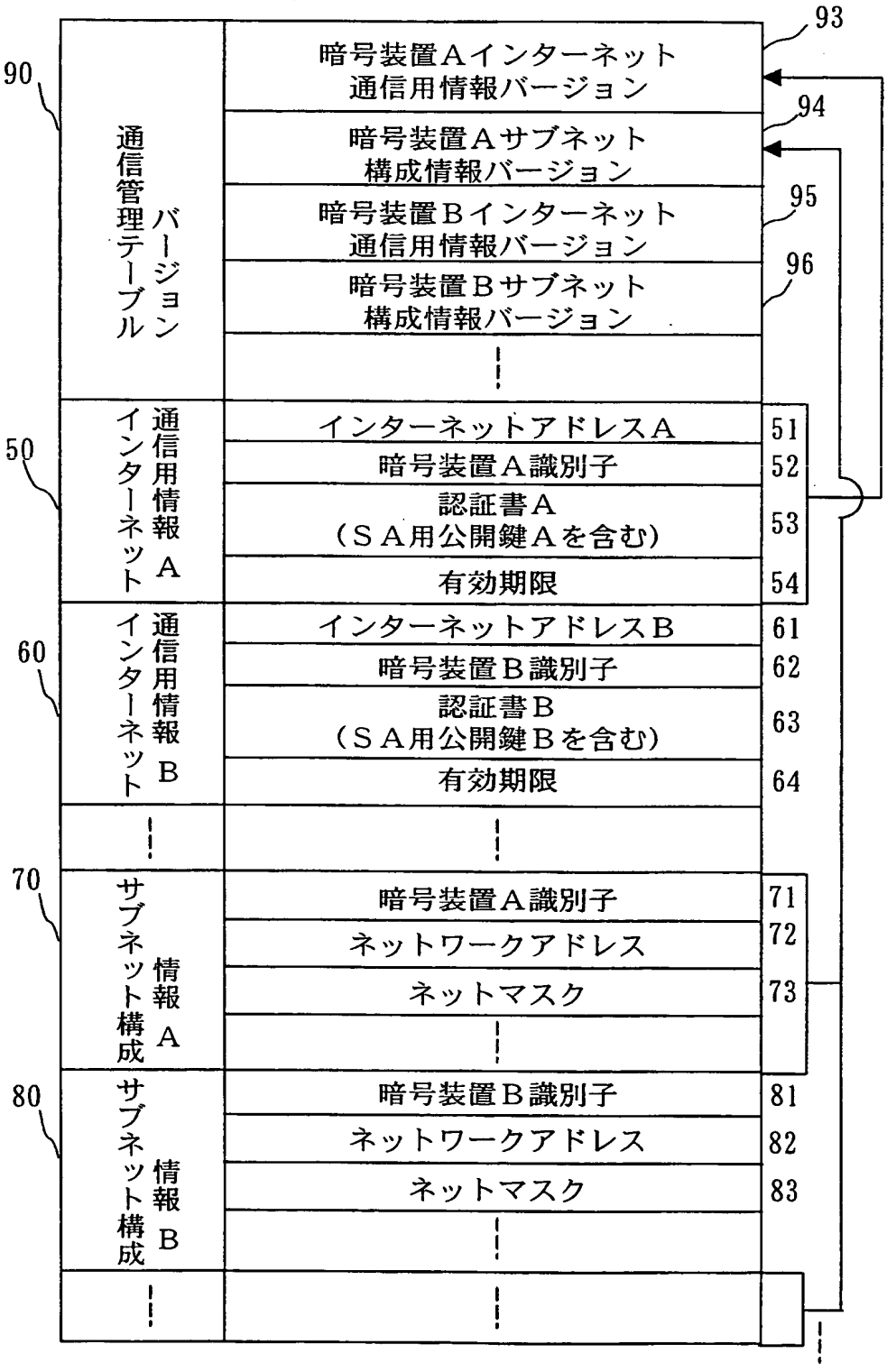

90
通信管理テーブル
バージョン
暗号装置Aインターネット通信用情報バージョン
93
暗号装置Aサブネット構成情報バージョン
94
暗号装置Bインターネット通信用情報バージョン
95
暗号装置Bサブネット構成情報バージョン
96
50
通信用情報A
インターネット
インターネットアドレスA
51
暗号装置A識別子
52
認証書A
（SA用公開鍵Aを含む）
53
有効期限
54
60
通信用情報B
インターネット
インターネットアドレスB
61
暗号装置B識別子
62
認証書B
（SA用公開鍵Bを含む）
63
有効期限
64
70
サブネット構成情報A
暗号装置A識別子
71
ネットワークアドレス
72
ネットマスク
73
80
サブネット構成情報B
暗号装置B識別子
81
ネットワークアドレス
82
ネットマスク
83

図 10

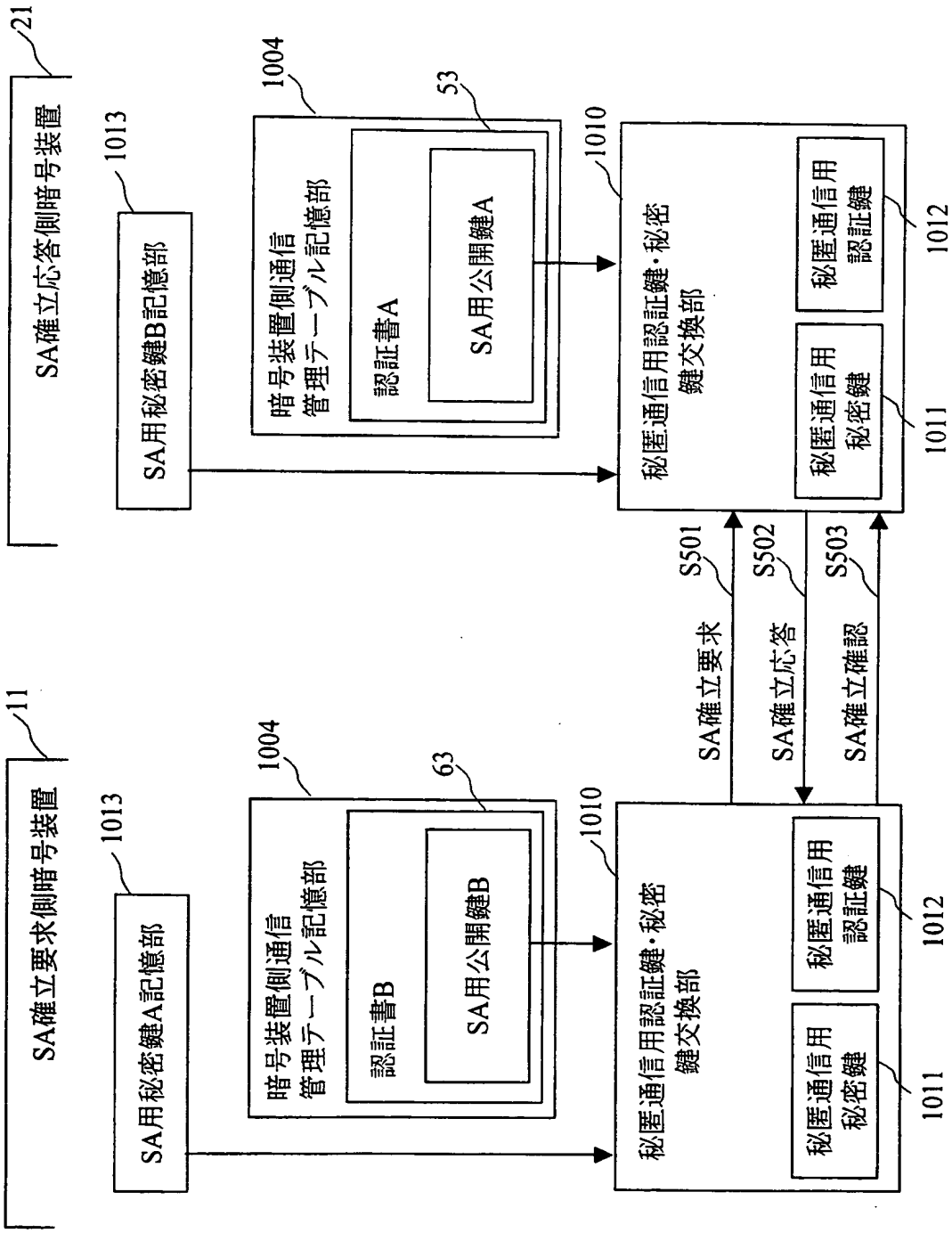

SA確立要求側暗号装置
11
SA用秘密鍵A記憶部
1013
暗号装置側通信
管理テーブル記憶部
1004
認証書B
SA用公開鍵B
63
秘匿通信用認証鍵・秘密
鍵交換部
1010
秘匿通信用
秘密鍵
秘匿通信用
認証鍵
1011
1012
SA確立応答側暗号装置
21
SA用秘密鍵B記憶部
1013
暗号装置側通信
管理テーブル記憶部
1004
認証書A
SA用公開鍵A
53
秘匿通信用認証鍵・秘密
鍵交換部
1010
秘匿通信用
秘密鍵
秘匿通信用
認証鍵
1011
1012
S501
SA確立要求
S502
SA確立応答
S503
SA確立確認

図 11

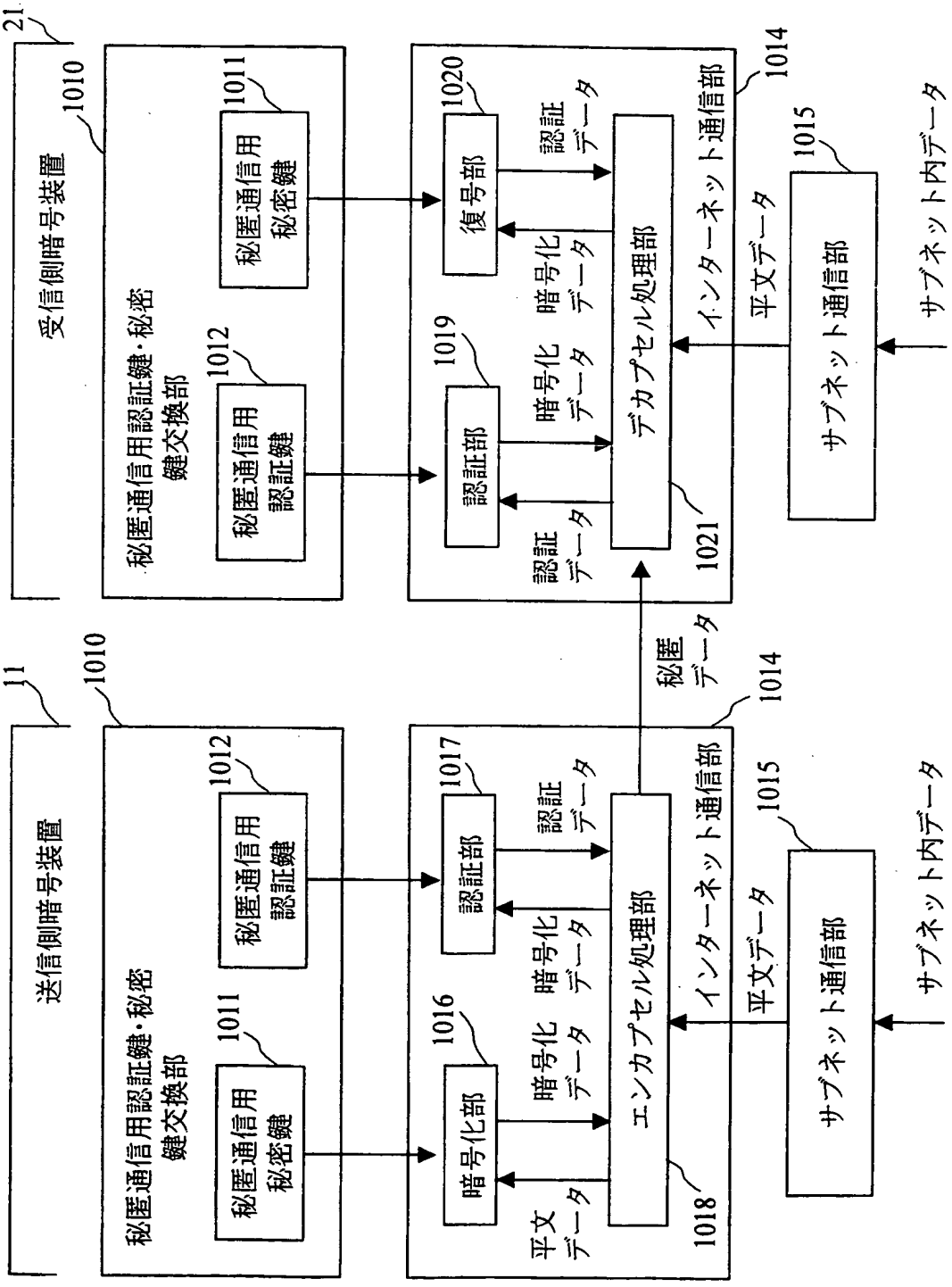

送信側暗号装置
11
1010
秘匿通信用認証鍵・秘密鍵交換部
1011
秘匿通信用秘密鍵
1012
秘匿通信用認証鍵
暗号化部
1016
認証部
1017
エンカプセル処理部
1018
インターネット通信部
1014
サブネット通信部
1015
サブネット内データ
平文データ
暗号化データ
認証データ
秘匿データ
受信側暗号装置
21
1010
秘匿通信用認証鍵・秘密鍵交換部
1011
秘匿通信用秘密鍵
1012
秘匿通信用認証鍵
復号部
1020
認証部
1019
デカプセル処理部
1021
インターネット通信部
1014
サブネット通信部
1015
サブネット内データ
平文データ
暗号化データ
認証データ

図 12

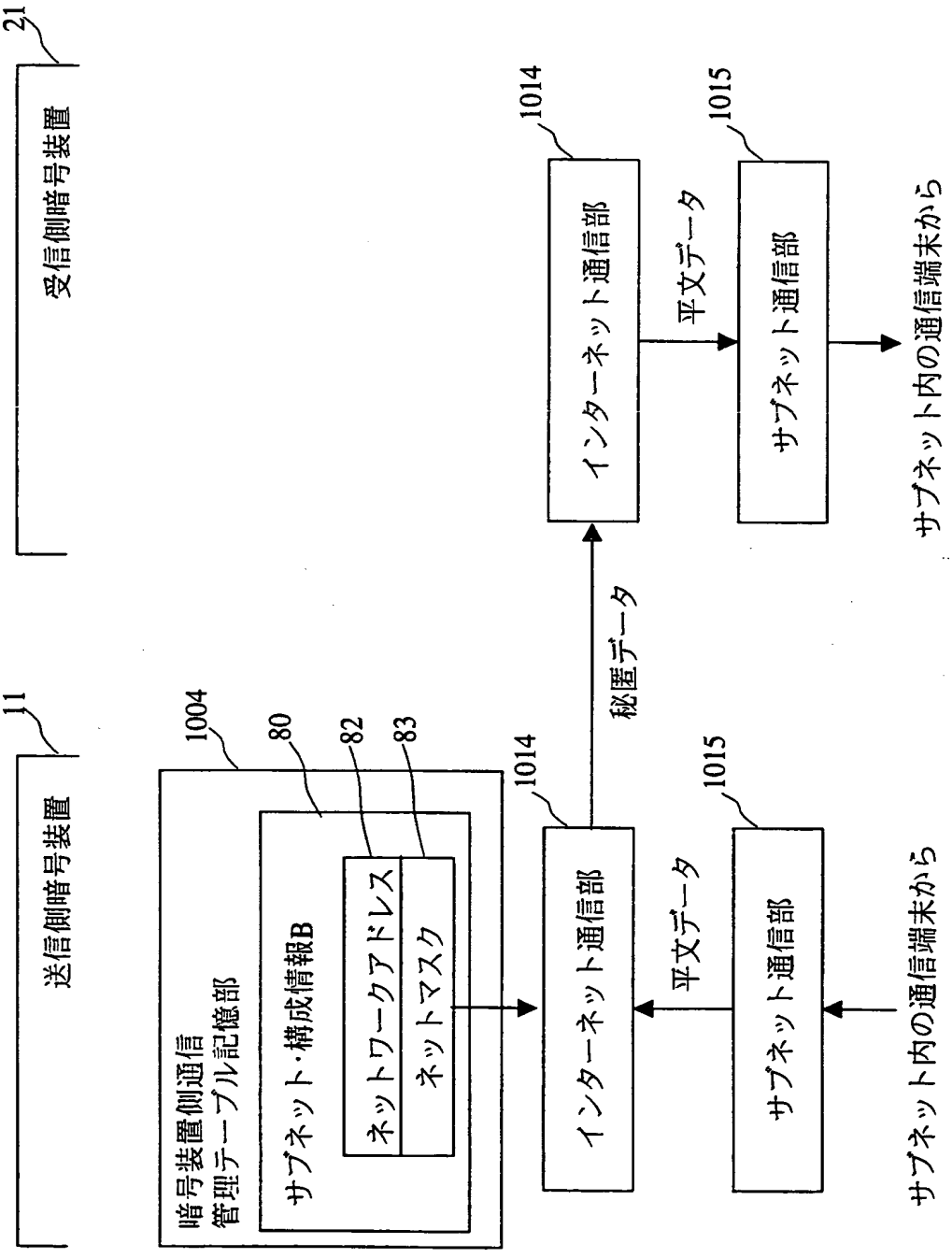

21
受信側暗号装置
1014
1015
インターネット通信部
平文データ
サブネット通信部
サブネット内の通信端末から
1004
80
82
83
暗号装置側通信
管理テーブル記憶部
サブネット・構成情報B
ネットワークアドレス
ネットマスク
秘匿データ
11
送信側暗号装置
1014
1015
インターネット通信部
平文データ
サブネット通信部
サブネット内の通信端末から

図 13

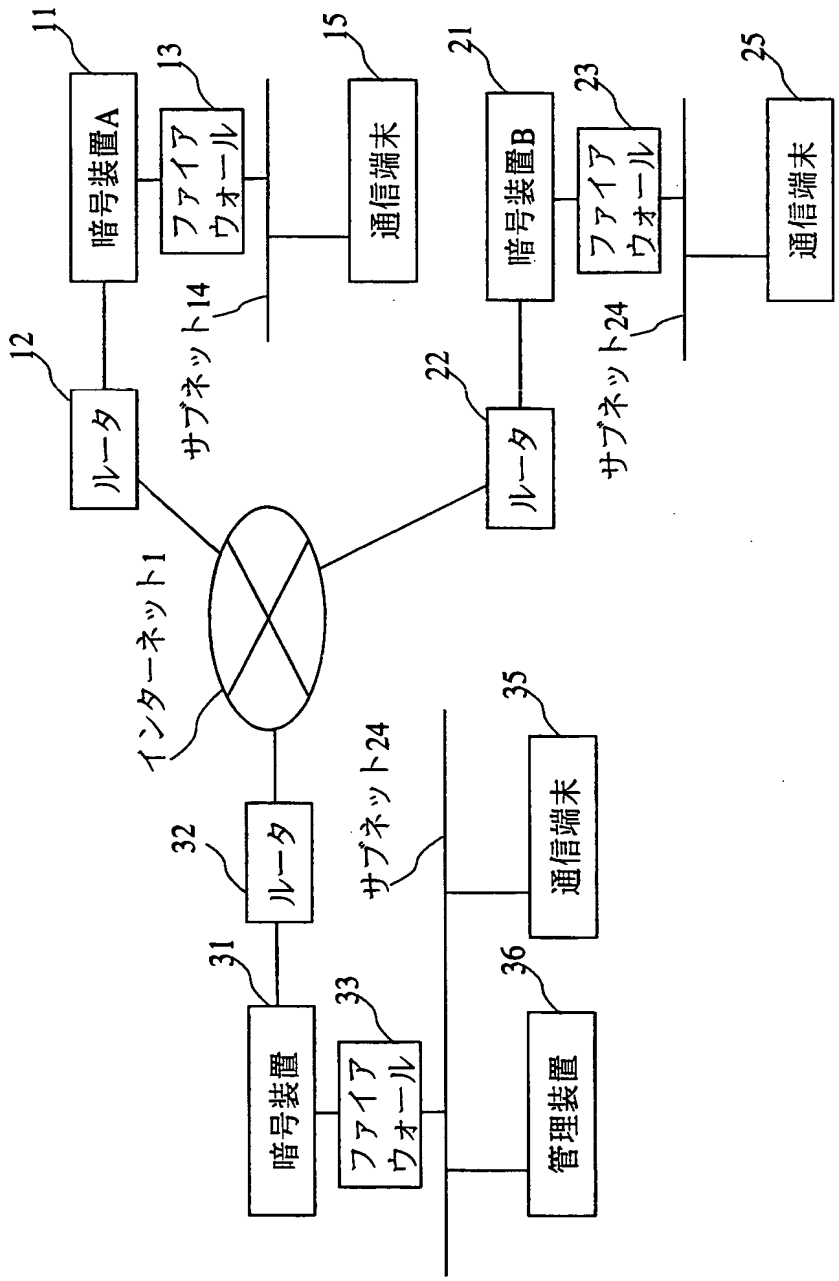

11
暗号装置A
13
ファイア
ウォール
15
通信端末
21
暗号装置B
23
ファイア
ウォール
25
通信端末
12
ルータ
サブネット14
22
ルータ
サブネット24
インターネット1
32
ルータ
サブネット24
35
通信端末
31
暗号装置
33
ファイア
ウォール
36
管理装置

図 14

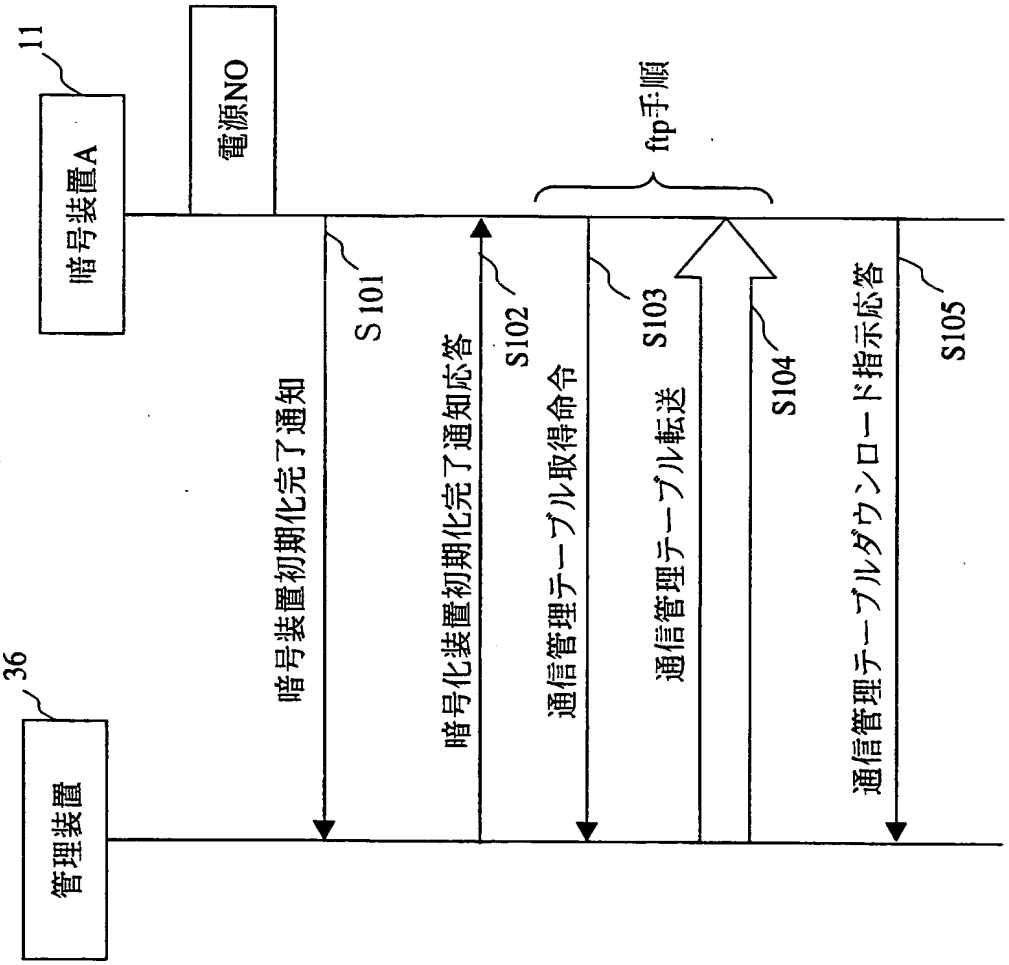
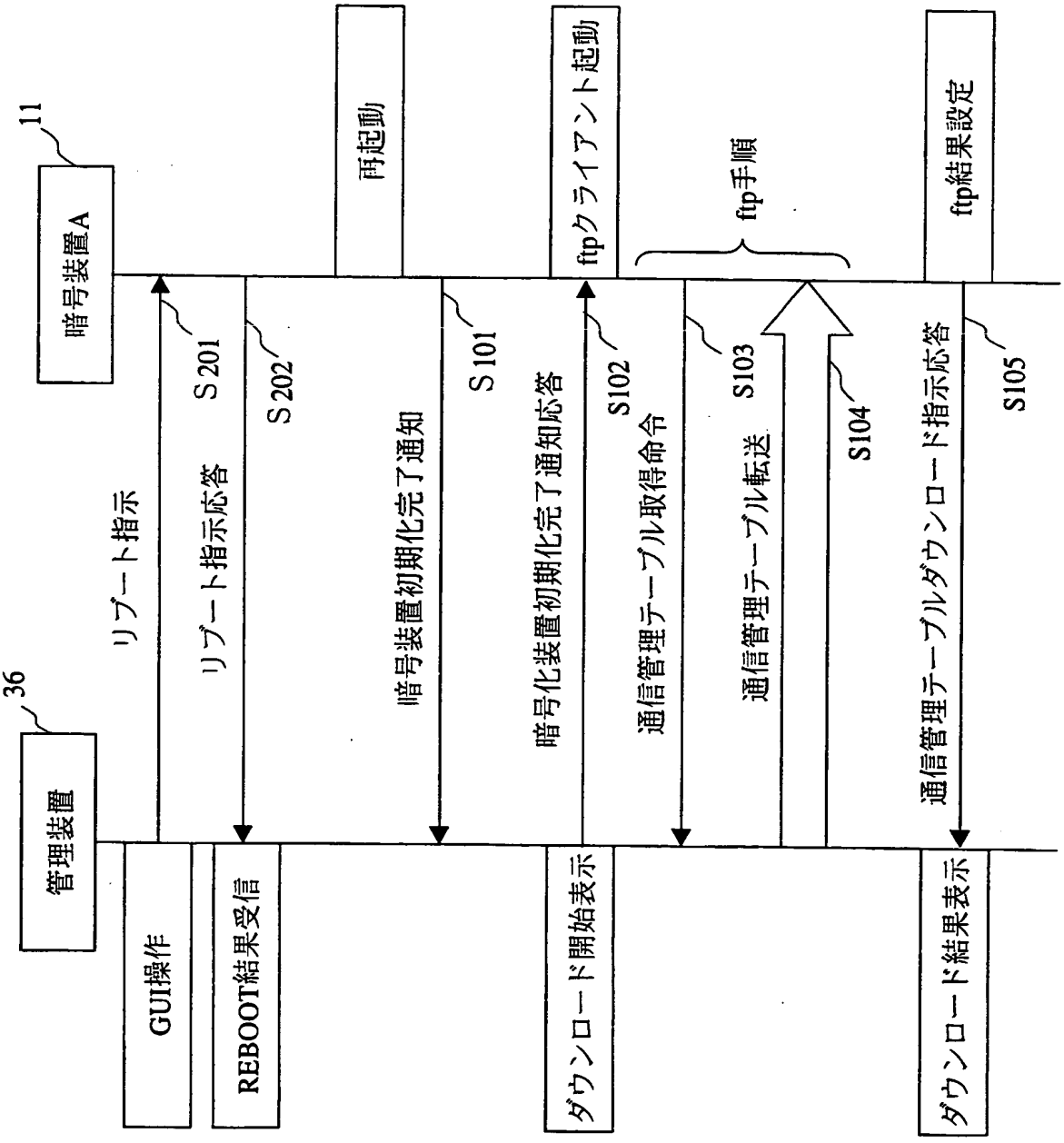

11
暗号装置A
電源NO
ftp手順
36
管理装置
暗号装置初期化完了通知
S101
暗号化装置初期化完了通知応答
S102
通信管理テーブル取得命令
S103
通信管理テーブル転送
S104
通信管理テーブルダウンロード指示応答
S105

図 15


管理装置
36
暗号装置A
11
GUI操作
リブート指示
REBOOT結果受信
リブート指示応答
S 201
再起動
S 202
暗号装置初期化完了通知
S 101
ダウンロード開始表示
暗号化装置初期化完了通知応答
S102
ftpクライアント起動
通信管理テーブル取得命令
S103
ftp手順
通信管理テーブル転送
S104
ダウンロード結果表示
通信管理テーブルダウンロード指示応答
S105
ftp結果設定

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/00474

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L 9/08, H04L 29/02

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G09C 1/00- 5/00, H04K 1/00-3/00, H04L 9/00, H04L 29/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JICST FILE (JOIS)
INSPEC (DIALOG)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Paul Albits and Criket Liu, Supervisors of translation: Hiroaki TAKADA, Ikuo KOJIMA; Translator: Mitsumasa KODATE, "DNS & BIND the 3rd ed.", the 2nd ed., Orairii Japan, (03 June, 1999), pp. vii-ix, 100-102	1-12
Y	RFC (Request for Comments) 2065, D. Eastlake, 3rd and C. Kaufman, "Domain Name System Security Extensions,"(Jan 1997)	1-12
A	RFC (Request for Comments) 1035, P. Mockapetris, "DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION,"(Nov 1987)	1-12

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 April, 2000 (13.04.00)	25 April, 2000 (25.04.00)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ００／００４７４

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））
Int.Cl⁷
Ｈ０４Ｌ　　９／０８
Ｈ０４Ｌ　２９／０２

Ｂ．　調査を行った分野
調査を行った最小限資料（国際特許分類（ＩＰＣ））
Int.Cl⁷
Ｇ０９Ｃ　１／００　－　５／００　　Ｈ０４Ｋ　１／００　－　３／００
Ｈ０４Ｌ　９／００　　Ｈ０４Ｌ　２９／００

最小限資料以外の資料で調査を行った分野に含まれるもの

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）
ＪＩＣＳＴファイル（ＪＯＩＳ）
ＩＮＳＰＥＣ（ＤＩＡＬＯＧ）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	Paul Albits and Criket Liu, 高田広章，小島育夫監訳，小舘光正訳， 「DNS & BIND 第３版」第２版，オライリー・ジャパン， (1999年6月3日)，pp. vii－ix，100－102	1-12
Y	RFC (Request for Comments) 2065, D. Eastlake, 3rd and C. Kaufman, "Domain Name System Security Extensions," (Jan 1997)	1-12
A	RFC (Request for Comments) 1035, P. Mockapetris, "DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION," (Nov 1987)	1-12

☐ Ｃ欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
１３．０４．００	25.04.00

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	
日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	丸山　高政	5W　９５７０
	電話番号　０３－３５８１－１１０１　内線　９５７０	

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（１９９８年７月）

明細書：　18頁
請求の範囲：　6頁
要約書：　1頁
} 計：25頁

明　細　書

通信管理テーブル転送システム及び管理装置及び暗号装置及び通信管理テーブル転送方法

技術分野

本発明は、インターネットを介して互いに接続する複数の暗号装置と、上記複数の暗号装置が通信に用いる通信管理テーブルを管理する管理装置とからなる通信管理テーブル転送システムに係り、セキュリティの向上と、性能の向上に関する。

背景技術

近年、仮想私設網（ＶＰＮ：Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）を用いるシステムが普及している。仮想私設網は、データの暗号化やユーザ認証などのセキュリティ技術を用いてインターネット等のパブリックネットワークを仮想的（Ｖｉｒｔｕａｌ）に専用線（Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）のように利用するネットワークのことである。仮想私設網によって、複数の組織における内部ネットワーク間を専用線を用いるかのごとく接続することができる。

図１３は、仮想私設網を用いるシステムの例を示す図である。１は、インターネット、１１、２１、３１は、暗号装置、１２、２２、３２は、ルータ、１３、２３、３３は、ファイアウォール、１４、２４、３４は、サブネット（内部ネットワーク）、１５、２５、３５は、通信端末、３６は、管理装置である。それぞれ、図のように接続されている。

インターネットを介したデータ転送を行なう場合、外部からの攻撃に対する防御手段としてＩＰ　ｓｅｃｕｒｕｔｙに準拠するシステムが用

いられる。ＩＰ　ｓｅｃｕｒｕｔｙは、インターネット通信規約標準化機関ＩＥＴＦ（Ｉｎｔｅｒｎｅｔ　Ｅｎｇｉｎｅｅｒｉｎｇ　Ｔａｓｋ　Ｆｏｒｃｅ）で定められたＩＰパケットレベルにおけるセキュリティ確保方式のことである。

ＩＰ　ｓｅｃｕｒｕｔｙでは、各内部ネットワーク上の暗号装置間で、ＳＡ（Ｓｅｃｕｒｉｔｙ　Ａｓｓｏｃｉａｔｉｏｎ）という関係を確立した上で、データの転送を行なう。これにより、秘匿通信が可能となる。しかし、ＳＡを確立する為には、その前提として公開鍵を暗号装置間で共有化しておく必要がある。

また、内部ネットワーク上の通信端末に対してデータを転送する場合には、各内部ネットワークの構成情報を知っておく必要もある。

そのため、上記の公開鍵や内部ネットワークの構成情報を含む通信管理テーブルを生成し、ＳＡの確立の前にこの通信管理テーブルを暗号装置間で交換する。このような通信管理テーブルを作成し、更新し、配信するために管理装置３６が設置される。

従来、暗号装置から通信管理テーブルを求められた管理装置３６は、無条件に通信管理テーブルを暗号装置へ配信していた。

図１４は、従来例における電源を入れたときの通信管理テーブルの転送の手順を示す図である。暗号装置Ａ１１の電源がいれられると、暗号装置Ａ１１は、暗号装置初期化通知（Ｓ１０１）を送信する。管理装置３６は、暗号装置初期化通知（Ｓ１０１）を受信すると、暗号装置初期化通知応答（Ｓ１０２）を送信する。暗号装置Ａ１１は、暗号装置初期化通知応答（Ｓ１０２）を受信すると無条件に通信管理テーブル取得命令（Ｓ１０３）を発行し、通信管理テーブル転送（Ｓ１０４）が行なわれる。

また、図１５は、従来例におけるリブートされたときの通信管理テー

ブルの転送の手順を示す図である。管理装置３６が、リブート指示（Ｓ２０１）を送信し、暗号装置Ａ１１が、リブート指示応答（Ｓ２０２）を送信した後、再起動する。これ以降、図１４と同様に動作する。

上述のシステムにおいては、通信管理テーブルの転送回数が多く、データ転送の性能を劣化させていた。

また、通信管理テーブルを盗用される機会を増加させ、セキュリティ上の問題があった。つまり、公開鍵や内部ネットワークの構成情報を盗まれ、暗号装置間のデータ転送の秘匿が守られないおそれがあった。

本発明は、上記した従来技術の欠点を除くためになされたものであって、通信管理テーブルの転送回数を減らし、データ転送の性能を向上させ、通信管理テーブルを盗用される機会を減らし、セキュリティを向上させることを目的とする。

発明の開示

この発明に係る通信管理テーブル転送システムは、インターネットを介して互いに接続する複数の暗号装置と、上記複数の暗号装置が通信に用いる通信管理テーブルを管理する管理装置とからなる通信管理テーブル転送システムであって、

上記暗号装置は、上記暗号装置で記憶する上記通信管理テーブルである暗号装置側通信管理テーブルを記憶する暗号装置側通信管理テーブル記憶部と、

上記暗号装置側通信管理テーブルのバージョンである暗号装置側通信管理テーブルバージョンを記憶する暗号装置側通信管理テーブルバージョン記憶部と、

上記暗号装置側通信管理テーブルバージョンを、上記管理装置へ送信する通信管理テーブルバージョン送信部とを備え、

上記管理装置は、上記管理装置で記憶する上記通信管理テーブルである管理装置側通信管理テーブルを記憶する管理装置側通信管理テーブル記憶部と、

上記管理装置側通信管理テーブルのバージョンである管理装置側通信管理テーブルバージョンを記憶する管理装置側通信管理テーブルバージョン記憶部と、

上記暗号装置から上記暗号装置側通信管理テーブルバージョンを受信する通信管理テーブルバージョン受信部と、

受信した上記暗号装置側通信管理テーブルバージョンと、上記管理装置側通信管理テーブルバージョンとの不一致を判定する通信管理テーブルバージョン判定部と、

上記通信管理テーブルバージョン判定部により不一致と判定された場合に、上記管理装置側通信管理テーブルを送信する通信管理テーブル送信部とを備え、

上記暗号装置は、更に、上記管理装置から上記管理装置側通信管理テーブルを受信する通信管理テーブル受信部を備え、

上記暗号装置側通信管理テーブル記憶部は、上記通信管理テーブル受信部により受信された上記管理装置側通信管理テーブルを、上記暗号装置側通信管理テーブルとして記憶することを特徴とする。

上記通信管理テーブル送信部は、上記通信管理テーブルバージョン判定部により不一致と判定された場合に、更に、上記管理装置側通信管理テーブルバージョンを送信し、

上記通信管理テーブル受信部は、更に、上記管理装置から上記管理装置側通信管理テーブルバージョンを受信し、

上記暗号装置側通信管理テーブルバージョン記憶部は、上記通信管理テーブル受信部により受信された上記管理装置側通信管理テーブルバー

ジョンを、上記暗号装置側通信管理テーブルバージョンとして記憶することを特徴とする。

この発明に係る管理装置は、インターネットを介して互いに接続する複数の暗号装置が通信に用いる通信管理テーブルを管理する管理装置であって、

上記管理装置で記憶する上記通信管理テーブルである管理装置側通信管理テーブルを記憶する管理装置側通信管理テーブル記憶部と、

上記管理装置側通信管理テーブルのバージョンである管理装置側通信管理テーブルバージョンを記憶する管理装置側通信管理テーブルバージョン記憶部と、

上記暗号装置から、上記暗号装置で記憶する上記通信管理テーブルである暗号装置側通信管理テーブルのバージョンである暗号装置側通信管理テーブルバージョンを受信する通信管理テーブルバージョン受信部と、

受信した上記暗号装置側通信管理テーブルバージョンと、上記管理装置側通信管理テーブルバージョンとの不一致を判定する通信管理テーブルバージョン判定部と、

上記通信管理テーブルバージョン判定部により不一致と判定された場合に、上記管理装置側通信管理テーブルを送信する通信管理テーブル送信部とを備えることを特徴とする。

上記通信管理テーブル送信部は、上記通信管理テーブルバージョン判定部により不一致と判定された場合に、更に、上記管理装置側通信管理テーブルバージョンを送信することを特徴とする。

上記管理装置は、更に、上記管理装置側通信管理テーブルと、上記管理装置側通信管理テーブルバージョンとを対応付けて更新する管理装置側通信管理テーブル更新部を有することを特徴とする。

上記管理装置は、更に、上記管理装置側通信管理テーブルの中で更新する情報である通信管理テーブル更新情報を受信する通信管理テーブル更新情報受信部を有することを特徴とする。

この発明に係る暗号装置は、インターネットを介して他の暗号装置と接続し、通信に用いる通信管理テーブルを管理装置によって管理される暗号装置であって、

上記暗号装置は、上記暗号装置で記憶する上記通信管理テーブルである暗号装置側通信管理テーブルを記憶する暗号装置側通信管理テーブル記憶部と、

上記暗号装置側通信管理テーブルのバージョンである暗号装置側通信管理テーブルバージョンを記憶する暗号装置側通信管理テーブルバージョン記憶部と、

上記暗号装置側通信管理テーブルバージョンを、上記管理装置へ送信する通信管理テーブルバージョン送信部と、

上記管理装置から、上記管理装置で記憶する上記通信管理テーブルである管理装置側通信管理テーブルを受信する通信管理テーブル受信部とを備え、

上記暗号装置側通信管理テーブル記憶部は、上記通信管理テーブル受信部により受信された上記管理装置側通信管理テーブルを、上記暗号装置側通信管理テーブルとして記憶することを特徴とする。

上記通信管理テーブル受信部は、更に、上記管理装置から上記管理装置側通信管理テーブルのバージョンである管理装置側通信管理テーブルバージョンを受信し、

上記暗号装置側通信管理テーブルバージョン記憶部は、上記通信管理テーブル受信部により受信された上記管理装置側通信管理テーブルバージョンを、上記暗号装置側通信管理テーブルバージョンとして記憶する

ことを特徴とする。

上記通信管理テーブルは、公開鍵を含み、

上記暗号装置は、更に、上記他の暗号装置と上記インターネットを介して秘匿通信を行なう際に用いる秘匿通信用秘密鍵を、上記暗号装置側通信管理テーブルに含まれる上記公開鍵を用いて上記他の暗号装置と共有化する秘匿鍵通信用秘密鍵交換部を備えることを特徴とする。

上記通信管理テーブルは、公開鍵を含み、

上記暗号装置は、更に、上記他の暗号装置と上記インターネットを介して秘匿通信を行なう際に用いる秘匿通信用認証鍵を、上記暗号装置側通信管理テーブルに含まれる上記公開鍵を用いて上記他の暗号装置と共有化する秘匿鍵通信用認証鍵交換部を備えることを特徴とする。

上記他の暗号装置は、サブネットに接続し、

上記通信管理テーブルは、上記サブネットの構成についての情報であるサブネット構成情報を含み、

上記暗号装置は、更に、上記暗号装置側通信管理テーブルに含まれる上記サブネット構成情報に基づいて、上記他の暗号装置と上記インターネットを介して通信を行なうインターネット通信部を有することを特徴とする。

この発明に係る通信管理テーブル転送方法は、インターネットを介して互いに接続し、それぞれ、暗号装置側通信管理テーブルを記憶する暗号装置側通信管理テーブル記憶部と、暗号装置側通信管理テーブルバージョンを記憶する暗号装置側通信管理テーブルバージョン記憶部とを有する複数の暗号装置と、

上記複数の暗号装置が通信に用いる通信管理テーブルを管理し、管理装置側通信管理テーブルを記憶する管理装置側通信管理テーブル記憶部と、管理装置側通信管理テーブルバージョンを記憶する管理装置側通信

管理テーブルバージョン記憶部とを有する管理装置とからなる通信管理テーブル転送システムの通信管理テーブル転送方法であって、

上記暗号装置が、上記暗号装置側通信管理テーブルバージョンを、上記管理装置へ送信する工程と、

上記管理装置が、上記暗号装置から上記暗号装置側通信管理テーブルバージョンを受信する工程と、

上記管理装置が、受信した上記暗号装置側通信管理テーブルバージョンと、上記管理装置側通信管理テーブルバージョンとの不一致を判定する工程と、

上記工程で不一致と判定した場合に、上記管理装置が、上記管理装置側通信管理テーブルを送信する工程と、

上記暗号装置が、上記管理装置から上記管理装置側通信管理テーブルを受信する工程と、

上記暗号装置が、受信した上記管理装置側通信管理テーブルを、上記暗号装置側通信管理テーブルとして記憶する工程とを有することを特徴とする。

図面の簡単な説明

図１は、本実施例における暗号装置の構成を示す図である。

図２は、本実施例における管理装置の構成を示す図である。

図３は、本実施例における電源を入れたときの通信管理テーブルの転送の手順を示す図である。

図４は、本実施例における電源を入れたときの通信管理テーブルの転送を省略する手順を示す図である。

図５は、本実施例におけるリブートされたときの通信管理テーブルの転送の手順を示す図である。

図６は、本実施例におけるリブートされたときの通信管理テーブルの転送を省略する手順を示す図である。

図７は、本実施例における通信管理テーブルの構成を示す図である。

図８は、本実施例における通信管理テーブルの構成を示す図である。

図９は、本実施例における通信管理テーブルの構成を示す図である。

図１０は、ＳＡ確立の際のデータフローを示す図である。

図１１は、秘匿通信の際のデータフローを示す図である。

図１２は、サブネット構成情報の使用例を示す図である。

図１３は、仮想私設網を用いるシステムの例を示す図である。

図１４は、従来例における電源を入れたときの通信管理テーブルの転送の手順を示す図である。

図１５は、従来例におけるリブートされたときの通信管理テーブルの転送の手順を示す図である。

発明を実施するための最良の形態

実施の形態１.

以下、本発明を図面に示す実施例に基づいて説明する。

図１は、本実施例における暗号装置の構成を示す図である。１００１は、電源制御部、１００２は、リブート制御部、１００３は、初期化部、１００４は、暗号装置側通信管理テーブル記憶部、１００５は、暗号装置側通信管理テーブルバージョン記憶部、１００６は、通信管理テーブルバージョン暗号化部、１００７は、初期化完了通知部、１００８は、通信管理テーブルダウンロード制御部、１００９は、通信管理テーブル受信部である。

図２は、本実施例における管理装置の構成を示す図である。２００１は、リブート指示部、２００２は、初期化完了受信部、２００３は、通

信管理テーブルバージョン復号部、２００４は、管理装置側通信管理テーブル記憶部、２００５は、管理装置側通信管理テーブルバージョン記憶部、２００６は、通信管理テーブルバージョン判定部、２００７は、通信管理テーブルダウンロード指示部、２００８は、通信管理テーブル送信部である。

図３は、本実施例おける電源を入れたときの通信管理テーブルの転送の手順を示す図である。以下、この手順について、図１及び図２の構成に基づいて説明する。

暗号装置Ａ１１側では、電源が入れられると、電源制御部１００１が初期化部１００３に初期化を指示する。初期化部１００３は、初期化を完了すると初期化完了通知部１００７に初期化の完了を知らせる。初期化完了通知部１００７は、管理装置３６の初期化完了受信部２００２に暗号装置初期化完了通知（Ｓ３０１）を送信する。このとき管理装置３６の公開鍵により暗号化した通信管理テーブルバージョンが、暗号装置初期化完了通知（Ｓ３０１）に含まれている。

通信管理テーブルバージョンは、暗号装置側通信管理テーブルバージョン記憶部１００５に記憶されている。暗号装置側通信管理テーブルバージョン記憶部１００５の通信管理テーブルバージョンは、暗号装置側通信管理テーブル記憶部１００４の通信管理テーブルと対応付けられている。この例では、暗号装置側通信管理テーブルバージョン記憶部１００５は、暗号装置側通信管理テーブル記憶部１００４に含まれるが、別個に設けても構わない。

通信管理テーブルバージョン暗号化部１００６は、暗号装置側通信管理テーブルバージョン記憶部１００５から通信管理テーブルバージョンを読み、これを暗号化し、暗号化された通信管理テーブルバージョンを初期化完了通知部１００７に送るように構成されている。

管理装置３６側では、初期化完了受信部２００２が、暗号装置初期化完了通知（Ｓ３０１）を受信し、通信管理テーブルバージョン復号部２００３が、暗号化されている通信管理テーブルバージョンを復号する。一方、通信管理テーブルバージョン判定部２００６は、管理装置側通信管理テーブルバージョン記憶部２００５から管理装置３６側で記憶する通信管理テーブルバージョンを読む。そして、通信管理テーブルバージョン判定部２００６は、これらの通信管理テーブルバージョンを比較する。尚、この実施例では、管理装置側通信管理テーブルバージョン記憶部２００５は、管理装置側通信管理テーブル記憶部２００４に含められているが、通信管理テーブルと通信管理テーブルバージョンが対応付けられていれば、別個に設けても構わない。

比較の結果、２つの通信管理テーブルバージョンが不一致の場合には、通信管理テーブルバージョン判定部２００６は、通信管理テーブルダウンロード指示部２００７に不一致を知らせる。

通信管理テーブルダウンロード指示部２００７は、不一致の知らせを受けると、暗号装置Ａ１１の通信管理テーブルダウンロード制御部１００８に通信管理テーブルダウンロード指示（Ｓ３０２）を送信する。

暗号装置Ａ１１側では、通信管理テーブルダウンロード制御部１００８が、通信管理テーブルダウンロード指示（Ｓ３０２）を受信するとファイル転送の手順に従って通信管理テーブルを受信する為に、通信管理テーブル受信部１００９に通信管理テーブル取得の指示を送る。

通信管理テーブル受信部１００９は、その指示を受けると、管理装置３６の通信管理テーブル送信部２００８に通信管理テーブル取得命令（Ｓ１０３）を送る。

管理装置３６側では、通信管理テーブル取得命令（Ｓ１０３）を受けた通信管理テーブル送信部２００８は、管理装置側通信管理テーブル記

憶部２００４から通信管理テーブルを読み、その通信管理テーブルを暗号装置Ａ１１の通信管理テーブル受信部１００９にファイル転送する（Ｓ１０４）。

暗号装置Ａ１１側では、通信管理テーブル受信部１００９が通信管理テーブルを受信し終えると、通信管理テーブルダウンロード制御部１００８に通信管理テーブル取得の完了を知らせ、通信管理テーブルダウンロード制御部１００８は通信管理テーブルダウンロード指示応答（Ｓ１０５）を管理装置３６の通信管理テーブルダウンロード指示部２００７に送信する。また、通信管理テーブル受信部１００９は、受信した通信管理テーブルを暗号装置側通信管理テーブル記憶部１００４に記憶する。

この例では、ファイル転送のときに通信管理テーブルに通信管理テーブルバージョンを含めて転送し、暗号装置側通信管理テーブル記憶部１００４は通信管理テーブルバージョンを含む通信管理テーブル記憶している。しかし、通信管理テーブルバージョンを、通信管理テーブルに含めない構成にすることもできる。つまり、通信管理テーブルバージョンを含まない通信管理テーブルと、通信管理テーブルバージョンを別個にファイル転送することも可能である。

このようにして、通信管理テーブルバージョンが一致しない場合は、通信管理テーブルが管理装置３６から暗号装置Ａ１１へ転送される。また、通信管理テーブルバージョンも転送される。

図４は、本実施例における電源を入れたときの通信管理テーブルの転送を省略する手順を示す図である。以下、この手順について、図１及び図２の構成に基づいて説明する。

通信管理テーブルバージョン判定部２００６が、通信管理テーブルバージョンを比較するまでの手順は、上述の手順と同様である。

比較の結果、通信管理テーブルバージョンが一致した場合には、通信管理テーブルバージョン判定部２００６は、一致を初期化完了受信部２００２に知らせる。

初期化完了受信部２００２は、暗号装置初期化完了通知応答（Ｓ１０２）を初期化完了通知部１００７に送信する。初期化完了通知部１００７が、暗号装置初期化完了通知応答（Ｓ１０２）を受け取ると動作を終了する。つまり、通信管理テーブルバージョンが一致する場合は、通信管理テーブルの転送は行なわれない。

暗号装置Ａ１１が通信管理テーブルバージョンを送信し、管理装置３６が通信管理テーブルバージョンを判定するタイミングは、初期化の時に限られない。システムで自由に設定することができる。例えば、リブートのタイミングや、定期的なタイミングであっても構わない。

図５は、本実施におけるリブートされたときの通信管理テーブルの転送の手順を示す図である。また、図６は、本実施におけるリブートされたときの通信管理テーブルの転送を省略する手順を示す図である。リブート指示（Ｓ２０１）とリブート指示応答（Ｓ２０２）に基づく再起動から始まる点を除き、図３及び図４の手順と同様である。

次に、通信管理テーブルの構成について説明する。図７、図８及び図９は本実施例における通信管理テーブルの構成を示す図である。

通信管理テーブルには、通信管理テーブルバージョン９０のほか、インターネット通信用情報Ａ５０、インターネット通信用情報Ｂ６０等のインターネット通信用情報と、サブネット構成情報Ａ７０、サブネット構成情報Ｂ８０等のサブネット構成情報が含まれる。

インターネット通信用情報Ａ５０は、暗号装置Ａ１１がインターネット１を介して、他の暗号装置と通信する場合に必要になる情報である。インターネット通信用情報Ｂ６０も同様に、暗号装置Ｂ２１がインター

ネット１を介して、他の暗号装置と通信する場合に必要になる情報である。

５１、６１は、インターネットアドレス、５２、６２は、暗号装置の識別子、５３、６３は、認証書、５４、６４は有効期限である。認証書には、ＳＡ用公開鍵が含まれている。

サブネット構成情報Ａ７０は、サブネット１４の構成に関する情報である。この図では、１レコードのみ示しているが、サブネット１４の構成に含まれる通信端末が多い場合には、更にレコードが付加されている。サブネット構成情報Ｂ８０も同様である。

７１、８１は、暗号装置の識別子、７２、８２は、ネットワークアドレス、７３、８３は、ネットマスクである。

図７の例では、通信管理テーブルバージョン９０は、バージョンは一つであり、通信管理テーブル全体の更新状況に対応している。

図８の例では、通信管理テーブルバージョン９０は、暗号装置Ａ情報バージョン９１、暗号装置Ｂ情報バージョン９２等複数のバージョンから構成されている。暗号装置Ａ情報バージョン９１は、インターネット通信用情報Ａ５０とサブネット構成情報Ａ７０等（サブネット構成情報Ａ７０の他にサブネット構成情報がある場合にはそれらも含む。）の更新状況に対応している。

図９の例では、更に細分化し、通信管理テーブルバージョン９０は、暗号装置Ａインターネット通信用情報バージョン９３、暗号装置Ａサブネット構成情報バージョン９４、暗号装置Ｂインターネット通信用情報バージョン９５、暗号装置Ｂサブネット構成情報バージョン９６等のバージョンから構成されている。暗号装置Ａインターネット通信用情報バージョン９３は、インターネット通信用情報Ａ５０の更新状況に対応している。また、暗号装置Ａサブネット構成情報バージョン９４は、サブ

ネット構成情報Ａ７０等（サブネット構成情報Ａ７０の他にサブネット構成情報がある場合にはそれらも含む。）の更新状況に対応している。

図８と図９の場合に、バージョンと各情報との対応をつけるために、各バージョンに対応して装置識別子や情報識別子を記憶する方法も考えられる。

管理装置３６は、各暗号装置から、通信管理テーブルの中で更新する情報である通信管理テーブル更新情報を受信する通信管理テーブル更新情報受信部（図示せず）と、管理装置側通信管理テーブルと、管理装置側通信管理テーブルバージョンとを対応付けて更新する管理装置側通信管理テーブル更新部（図示せず）を有する。

図７の場合、通信管理テーブル更新情報受信部は、いずれの暗号装置から通信管理テーブル更新情報を受信した場合にも、通信管理テーブルバージョン９０を更新する。図８の場合、通信管理テーブル更新情報受信部は、暗号装置Ａ１１から通信管理テーブル更新情報を受信した場合には、インターネット通信用情報Ａ５０、サブネット構成情報Ａ７０のいずれか若しくは両方を更新し、更に暗号装置Ａ情報バージョン９１を更新する。図９の場合、通信管理テーブル更新情報受信部は、暗号装置Ａ１１から通信管理テーブル更新情報を受信した場合には、インターネット通信用情報Ａ５０に関する通信管理テーブル更新情報、サブネット構成情報Ａ７０に関する通信管理テーブル更新情報のいずれか若しくは両方かを判断し、その部分を更新し、更にその部分に対応する暗号装置Ａインターネット通信用情報バージョン９３、暗号装置Ａサブネット構成情報バージョン９４のいずれか若しくは両方を更新する。

図８や図９のように、通信管理テーブルバージョンを細分化した場合には、通信管理テーブルバージョン判定部２００６は、細分化したバージョン毎に比較し、通信管理テーブルのうち不一致のバージョンに関す

る部分のみを通信管理テーブル転送（Ｓ１０４）で転送するようにすることも有効である。その場合は、通信管理テーブルダウンロード指示（Ｓ３０２）に転送する部分を特定する情報を付加し、通信管理テーブル受信部１００９は、暗号装置側通信管理テーブル記憶部１００４の中のその部分のみを更新し、暗号装置側通信管理テーブルバージョン記憶部１００５の中のその部分のバージョンのみを更新する。

次に、通信管理テーブルに含まれるＳＡ用公開鍵を用いてＳＡを確立する動作について説明する。図１０は、ＳＡ確立の際のデータフローを示す図である。この例では、暗号装置Ａ１１がＳＡ確立を要求する側であり、暗号装置Ｂ２１がＳＡ確立の要求に応答する側である。それぞれの暗号装置は、自らのＳＡ用秘密鍵を記憶するＳＡ用秘密鍵記憶部１０１３と、秘匿通信用秘密鍵１０１１と秘匿通信用認証鍵１０１２を共有化する秘匿通信用認証鍵秘密鍵交換部１０１０とを有する。秘匿通信用認証鍵秘密鍵交換部１０１０は、図に示すように、自らのＳＡ用秘密鍵と、相手側のＳＡ用公開鍵とを入力できるように構成されている。

暗号装置Ａ１１の秘匿通信用認証鍵秘密鍵交換部１０１０は、乱数Ｘａを生成し、署名し、暗号化し、暗号装置Ｂ２１側へ送信する（Ｓ５０１）。暗号装置Ｂ２１の秘匿通信用認証鍵秘密鍵交換部１０１０は、乱数Ｘｂを生成し、乱数Ｘａと組合わせて秘匿通信用秘密鍵１０１１と秘匿通信用認証鍵１０１２を生成する。更に、ＸｂとＸａのハッシュ値を署名し、暗号化し、暗号装置Ａ１１側へ送信する（Ｓ５０２）。暗号装置Ａ１１の秘匿通信用認証鍵秘密鍵交換部１０１０は、乱数Ｘａと乱数Ｘｂとを組合わせて秘匿通信用秘密鍵１０１１と秘匿通信用認証鍵１０１２を生成し、受信したハッシュ値を検証する。更に乱数Ｘｂのハッシュ値を暗号装置Ｂ２１側に送信する（Ｓ５０３）。暗号装置Ｂ２１の秘匿通信用認証鍵秘密鍵交換部１０１０は、受信したハッシュ値を検証す

る。以上の手順により、ＳＡが確立する。これによって、両者は、共通の秘匿通信用秘密鍵１０１１と秘匿通信用認証鍵１０１２を取得する。

次に、ＳＡ確立の後に行われる秘匿通信の動作について説明する。図１１は、秘匿通信の際のデータフローを示す図である。この例では、暗号装置Ａ１１がデータを送信する側であり、暗号装置Ｂ２１がデータを受信する側である。但し、ＳＡが確立している暗号装置間では、双方向の通信が可能であり、この例に限定されない。

それぞれの暗号装置は、インターネット通信部１０１４と、サブネット通信部１０１５とを有する。インターネット通信部１０１４は、インターネット１を介する通信を制御し、サブネット通信部１０１５は、サブネットを介する通信を制御する。

送信側のインターネット通信部１０１４は、暗号化部１０１６と、認証部１０１７と、エンカプセル処理部１０１８が動作する。また、受信側のインターネット通信部１０１４は、認証部１０１９と、復号部１０２０と、デカプセル処理部１０２１が動作する。この動作において、秘匿通信用秘密鍵１０１１は、暗号アルゴリズムに使用され、秘匿通信用認証鍵１０１２は、認証アルゴリズムに使用される。

また、通信管理テーブルに含まれるサブネット構成情報は、他の暗号装置に接続されるサブネットに対して通信を行なう場合に用いられる。図１２に示すように、サブネット構成情報は、インターネット通信部１０１４で用いられる。

産業上の利用可能性

本発明においては、管理装置と暗号装置の間で、通信管理テーブルのバージョンを管理し、両者間の通信管理テーブルの同一性が確認できた場合には、通信管理テーブルの転送を行なわないように構成したので、

通信管理テーブルの転送回数が削減され、データ通信の性能及び安全性が著しく向上する。

請求の範囲

1．インターネットを介して互いに接続する複数の暗号装置と、上記複数の暗号装置が通信に用いる通信管理テーブルを管理する管理装置とからなる通信管理テーブル転送システムであって、

上記暗号装置は、上記暗号装置で記憶する上記通信管理テーブルである暗号装置側通信管理テーブルを記憶する暗号装置側通信管理テーブル記憶部と、

上記暗号装置側通信管理テーブルのバージョンである暗号装置側通信管理テーブルバージョンを記憶する暗号装置側通信管理テーブルバージョン記憶部と、

上記暗号装置側通信管理テーブルバージョンを、上記管理装置へ送信する通信管理テーブルバージョン送信部とを備え、

上記管理装置は、上記管理装置で記憶する上記通信管理テーブルである管理装置側通信管理テーブルを記憶する管理装置側通信管理テーブル記憶部と、

上記管理装置側通信管理テーブルのバージョンである管理装置側通信管理テーブルバージョンを記憶する管理装置側通信管理テーブルバージョン記憶部と、

上記暗号装置から上記暗号装置側通信管理テーブルバージョンを受信する通信管理テーブルバージョン受信部と、

受信した上記暗号装置側通信管理テーブルバージョンと、上記管理装置側通信管理テーブルバージョンとの不一致を判定する通信管理テーブルバージョン判定部と、

上記通信管理テーブルバージョン判定部により不一致と判定された場合に、上記管理装置側通信管理テーブルを送信する通信管理テーブル送

信部とを備え、

上記暗号装置は、更に、上記管理装置から上記管理装置側通信管理テーブルを受信する通信管理テーブル受信部を備え、

上記暗号装置側通信管理テーブル記憶部は、上記通信管理テーブル受信部により受信された上記管理装置側通信管理テーブルを、上記暗号装置側通信管理テーブルとして記憶することを特徴とする通信管理テーブル転送システム。

2．上記通信管理テーブル送信部は、上記通信管理テーブルバージョン判定部により不一致と判定された場合に、更に、上記管理装置側通信管理テーブルバージョンを送信し、

上記通信管理テーブル受信部は、更に、上記管理装置から上記管理装置側通信管理テーブルバージョンを受信し、

上記暗号装置側通信管理テーブルバージョン記憶部は、上記通信管理テーブル受信部により受信された上記管理装置側通信管理テーブルバージョンを、上記暗号装置側通信管理テーブルバージョンとして記憶することを特徴とする請求項１記載の通信管理テーブル転送システム。

3．インターネットを介して互いに接続する複数の暗号装置が通信に用いる通信管理テーブルを管理する管理装置であって、

上記管理装置で記憶する上記通信管理テーブルである管理装置側通信管理テーブルを記憶する管理装置側通信管理テーブル記憶部と、

上記管理装置側通信管理テーブルのバージョンである管理装置側通信管理テーブルバージョンを記憶する管理装置側通信管理テーブルバージョン記憶部と、

上記暗号装置から、上記暗号装置で記憶する上記通信管理テーブルである暗号装置側通信管理テーブルのバージョンである暗号装置側通信管理テーブルバージョンを受信する通信管理テーブルバージョン受信部と

受信した上記暗号装置側通信管理テーブルバージョンと、上記管理装置側通信管理テーブルバージョンとの不一致を判定する通信管理テーブルバージョン判定部と、

上記通信管理テーブルバージョン判定部により不一致と判定された場合に、上記管理装置側通信管理テーブルを送信する通信管理テーブル送信部とを備えることを特徴とする管理装置。

4．上記通信管理テーブル送信部は、上記通信管理テーブルバージョン判定部により不一致と判定された場合に、更に、上記管理装置側通信管理テーブルバージョンを送信することを特徴とする請求項3記載の管理装置。

5．上記管理装置は、更に、上記管理装置側通信管理テーブルと、上記管理装置側通信管理テーブルバージョンとを対応付けて更新する管理装置側通信管理テーブル更新部を有することを特徴とする請求項3記載の管理装置。

6．上記管理装置は、更に、上記管理装置側通信管理テーブルの中で更新する情報である通信管理テーブル更新情報を受信する通信管理テーブル更新情報受信部を有することを特徴とする請求項5記載の管理装置。

7．インターネットを介して他の暗号装置と接続し、通信に用いる通信管理テーブルを管理装置によって管理される暗号装置であって、

上記暗号装置は、上記暗号装置で記憶する上記通信管理テーブルである暗号装置側通信管理テーブルを記憶する暗号装置側通信管理テーブル記憶部と、

上記暗号装置側通信管理テーブルのバージョンである暗号装置側通信

管理テーブルバージョンを記憶する暗号装置側通信管理テーブルバージョン記憶部と、

上記暗号装置側通信管理テーブルバージョンを、上記管理装置へ送信する通信管理テーブルバージョン送信部と、

上記管理装置から、上記管理装置で記憶する上記通信管理テーブルである管理装置側通信管理テーブルを受信する通信管理テーブル受信部とを備え、

上記暗号装置側通信管理テーブル記憶部は、上記通信管理テーブル受信部により受信された上記管理装置側通信管理テーブルを、上記暗号装置側通信管理テーブルとして記憶することを特徴とする暗号装置。

8．上記通信管理テーブル受信部は、更に、上記管理装置から上記管理装置側通信管理テーブルのバージョンである管理装置側通信管理テーブルバージョンを受信し、

上記暗号装置側通信管理テーブルバージョン記憶部は、上記通信管理テーブル受信部により受信された上記管理装置側通信管理テーブルバージョンを、上記暗号装置側通信管理テーブルバージョンとして記憶することを特徴とする請求項７記載の暗号装置。

9．上記通信管理テーブルは、公開鍵を含み、

上記暗号装置は、更に、上記他の暗号装置と上記インターネットを介して秘匿通信を行なう際に用いる秘匿通信用秘密鍵を、上記暗号装置側通信管理テーブルに含まれる上記公開鍵を用いて上記他の暗号装置と共有化する秘匿鍵通信用秘密鍵交換部を備えることを特徴とする請求項７記載の暗号装置。

１０．上記通信管理テーブルは、公開鍵を含み、

上記暗号装置は、更に、上記他の暗号装置と上記インターネットを介して秘匿通信を行なう際に用いる秘匿通信用認証鍵を、上記暗号装置側

通信管理テーブルに含まれる上記公開鍵を用いて上記他の暗号装置と共有化する秘匿鍵通信用認証鍵交換部を備えることを特徴とする請求項７記載の暗号装置。

１１．上記他の暗号装置は、サブネットに接続し、

上記通信管理テーブルは、上記サブネットの構成についての情報であるサブネット構成情報を含み、

上記暗号装置は、更に、上記暗号装置側通信管理テーブルに含まれる上記サブネット構成情報に基づいて、上記他の暗号装置と上記インターネットを介して通信を行なうインターネット通信部を有することを特徴とする請求項７記載の暗号装置。

１２．インターネットを介して互いに接続し、それぞれ、暗号装置側通信管理テーブルを記憶する暗号装置側通信管理テーブル記憶部と、暗号装置側通信管理テーブルバージョンを記憶する暗号装置側通信管理テーブルバージョン記憶部とを有する複数の暗号装置と、

上記複数の暗号装置が通信に用いる通信管理テーブルを管理し、管理装置側通信管理テーブルを記憶する管理装置側通信管理テーブル記憶部と、管理装置側通信管理テーブルバージョンを記憶する管理装置側通信管理テーブルバージョン記憶部とを有する管理装置とからなる通信管理テーブル転送システムの通信管理テーブル転送方法であって、

上記暗号装置が、上記暗号装置側通信管理テーブルバージョンを、上記管理装置へ送信する工程と、

上記管理装置が、上記暗号装置から上記暗号装置側通信管理テーブルバージョンを受信する工程と、

上記管理装置が、受信した上記暗号装置側通信管理テーブルバージョンと、上記管理装置側通信管理テーブルバージョンとの不一致を判定する工程と、

上記工程で不一致と判定した場合に、上記管理装置が、上記管理装置側通信管理テーブルを送信する工程と、

上記暗号装置が、上記管理装置から上記管理装置側通信管理テーブルを受信する工程と、

上記暗号装置が、受信した上記管理装置側通信管理テーブルを、上記暗号装置側通信管理テーブルとして記憶する工程とを有することを特徴とする通信管理テーブル転送方法。

要　約　書

インターネットを介して互いに接続する複数の暗号装置と、上記複数の暗号装置が通信に用いる通信管理テーブルを管理する管理装置とからなる通信管理テーブル転送システムに係り、セキュリティの向上と、性能の向上とを図ることを課題とする。

管理装置３６は、暗号装置１１から通信管理テーブルバージョンを受信し（Ｓ３０１）、通信管理テーブルバージョン判定部２００６で、管理装置側通信管理テーブルバージョン記憶部２００５に記憶している通信管理テーブルバージョンと比較し、不一致の場合にのみ暗号装置１１に対して通信管理テーブルを転送する（Ｓ１０４）。

図 1

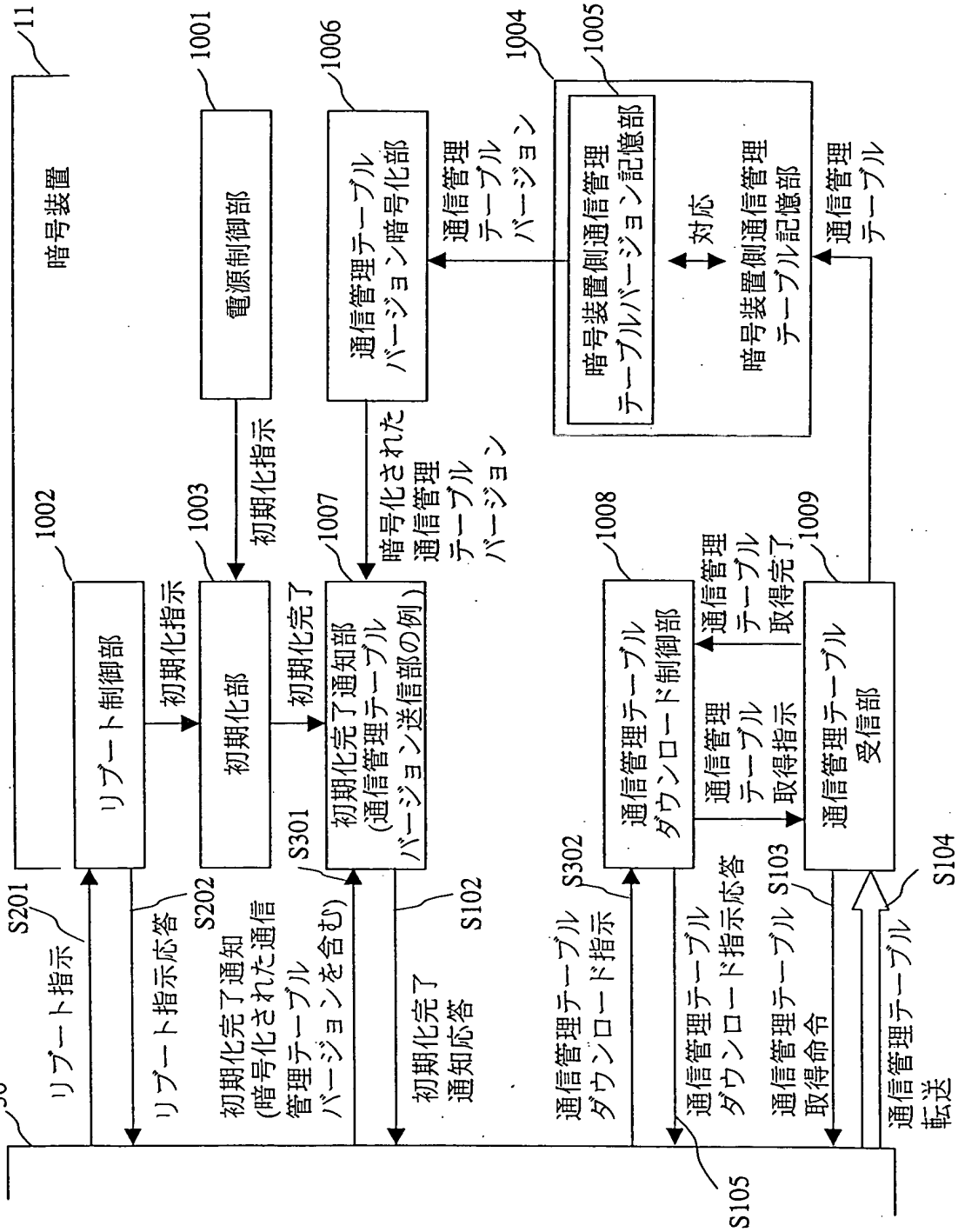


図 2

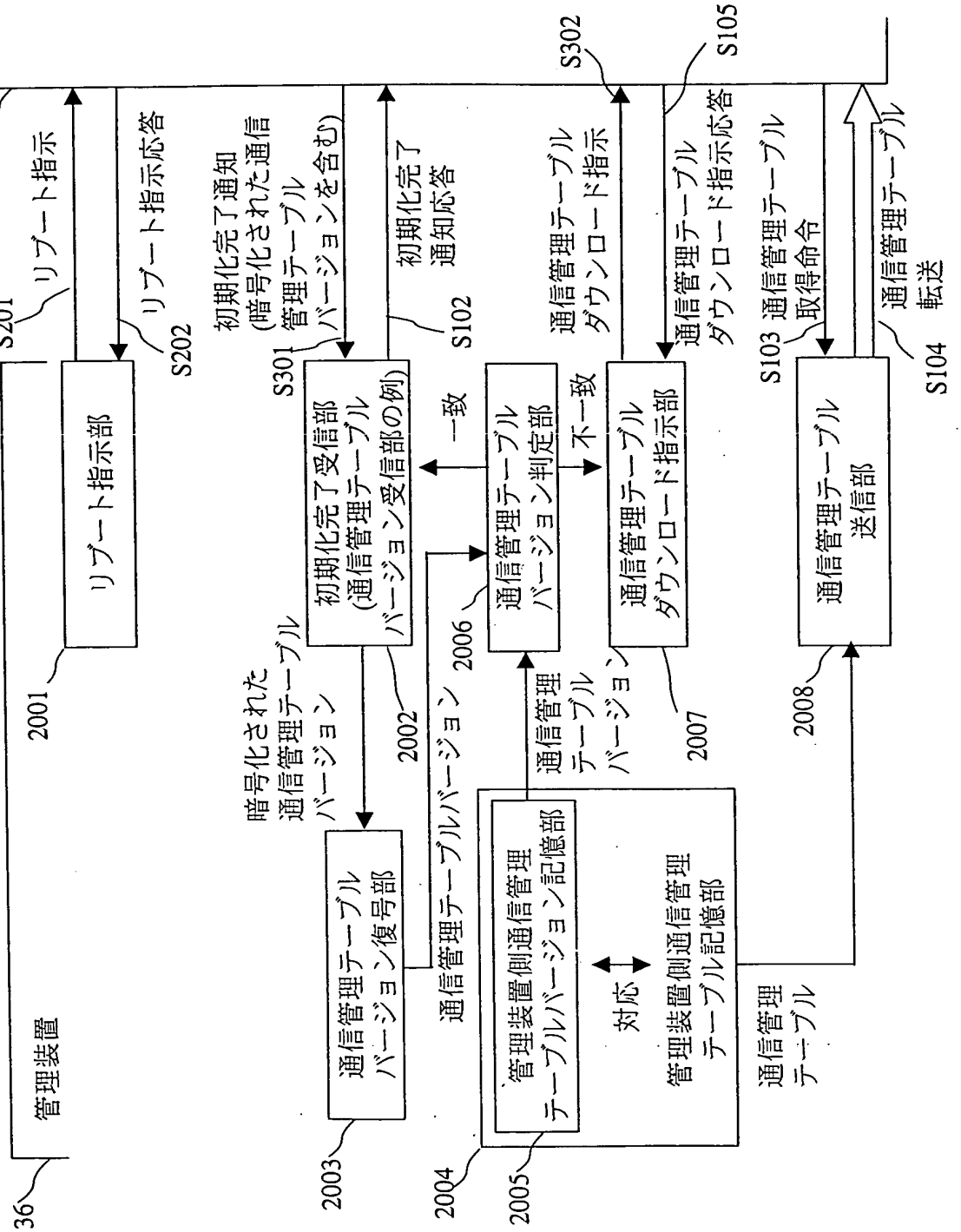

11
S201
リブート指示
S202
リブート指示応答
初期化完了通知
(暗号化された通信
管理テーブル
バージョンを含む)
S301
初期化完了
通知応答
S102
通信管理テーブル
ダウンロード指示
S302
通信管理テーブル
ダウンロード指示応答
S105
S103 通信管理テーブル
取得命令
S104 通信管理テーブル
転送
管理装置
リブート指示部
2001
初期化完了受信部
(通信管理テーブル
バージョン受信部の例)
一致
不一致
通信管理テーブル
バージョン判定部
通信管理テーブル
ダウンロード指示部
通信管理テーブル
送信部
暗号化された
通信管理テーブル
バージョン
2002
通信管理テーブルバージョン
2006
通信管理
テーブル
バージョン
2007
2008
通信管理テーブル
バージョン復号部
2003
管理装置側通信管理
テーブルバージョン記憶部
2004
2005
対応
管理装置側通信管理
テーブル記憶部
通信管理
テーブル
36

図 3

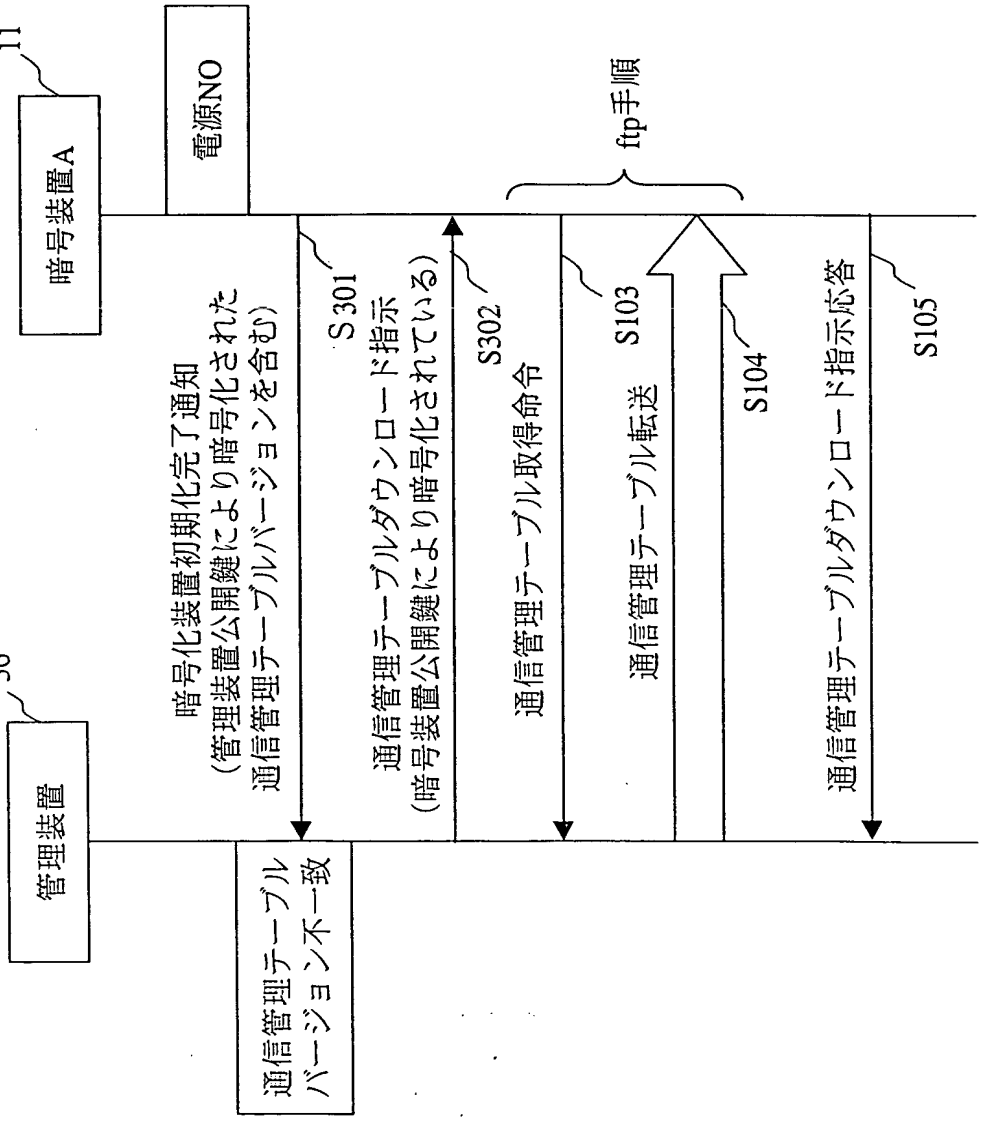

11
暗号装置A
電源NO
ftp手順
暗号化装置初期化完了通知
(管理装置公開鍵により暗号化された
通信管理テーブルバージョンを含む)
S301
通信管理テーブルダウンロード指示
(暗号装置公開鍵により暗号化されている)
S302
通信管理テーブル取得命令
S103
通信管理テーブル転送
S104
通信管理テーブルダウンロード指示応答
S105
36
管理装置
通信管理テーブル
バージョン不一致

図 4

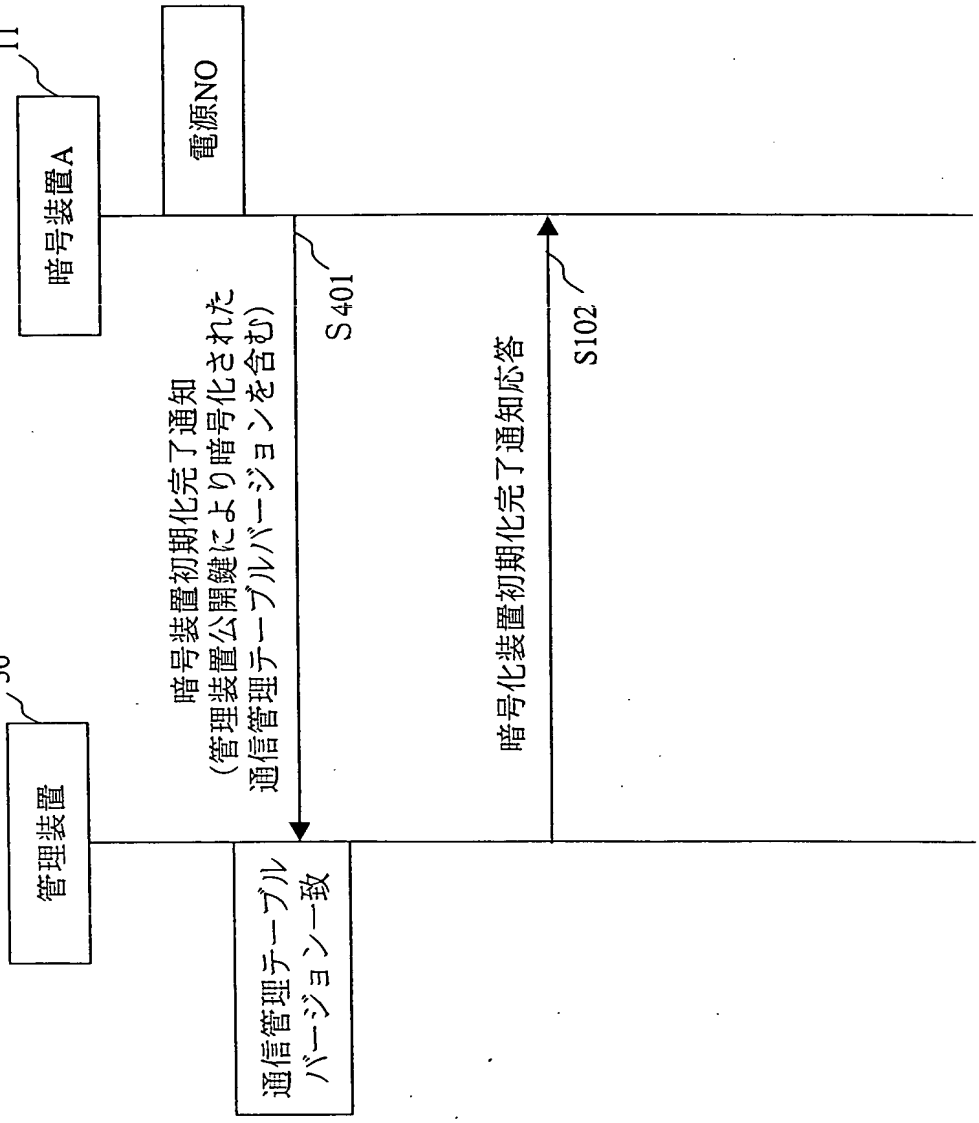

11
暗号装置A
電源NO
36
管理装置
通信管理テーブル
バージョン一致
暗号装置初期化完了通知
(管理装置公開鍵により暗号化された
通信管理テーブルバージョンを含む)
S401
暗号化装置初期化完了通知応答
S102

図 5

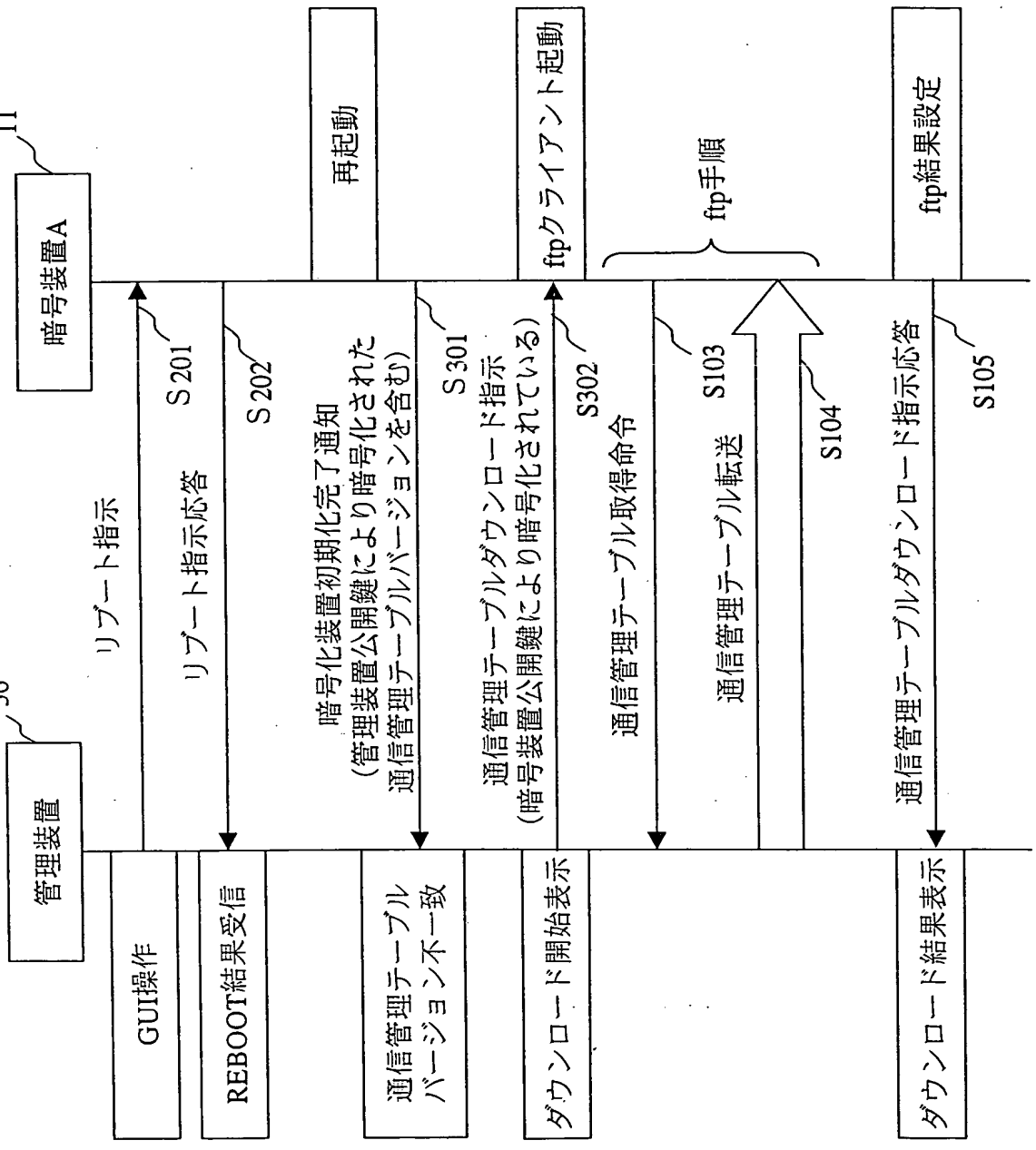

管理装置
36
暗号装置A
11
GUI操作
リブート指示
REBOOT結果受信
リブート指示応答
S201
再起動
S202
通信管理テーブル
バージョン不一致
暗号化装置初期化完了通知
(管理装置公開鍵により暗号化された
通信管理テーブルバージョンを含む)
S301
ダウンロード開始表示
通信管理テーブルダウンロード指示
(暗号装置公開鍵により暗号化されている)
S302
ftpクライアント起動
ftp手順
通信管理テーブル取得命令
S103
通信管理テーブル転送
S104
ftp結果設定
ダウンロード結果表示
通信管理テーブルダウンロード指示応答
S105

図 6

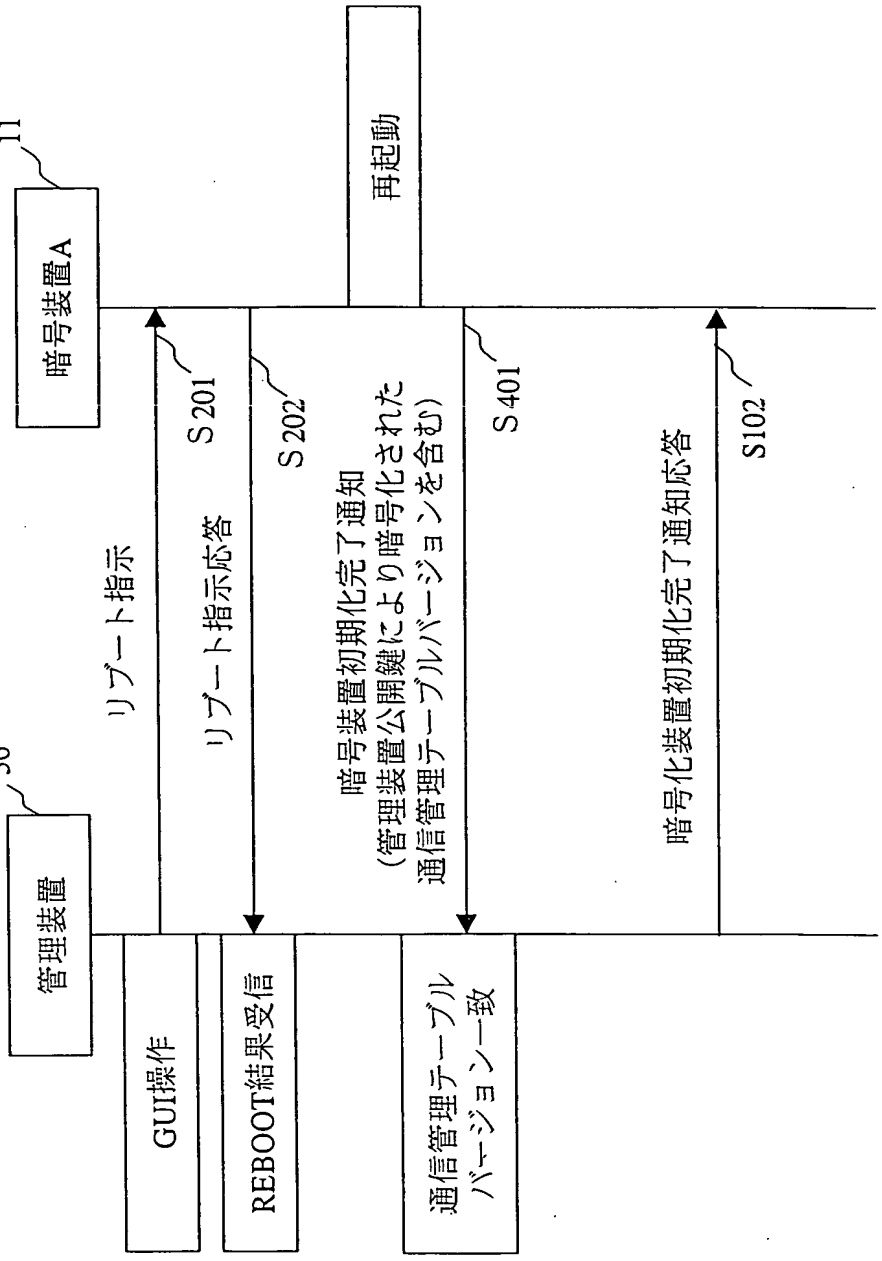

11
暗号装置A
再起動
リブート指示
S201
リブート指示応答
S202
暗号装置初期化完了通知
(管理装置公開鍵により暗号化された
通信管理テーブルバージョンを含む)
S401
暗号化装置初期化完了通知応答
S102
36
管理装置
GUI操作
REBOOT結果受信
通信管理テーブル
バージョン一致

図 7

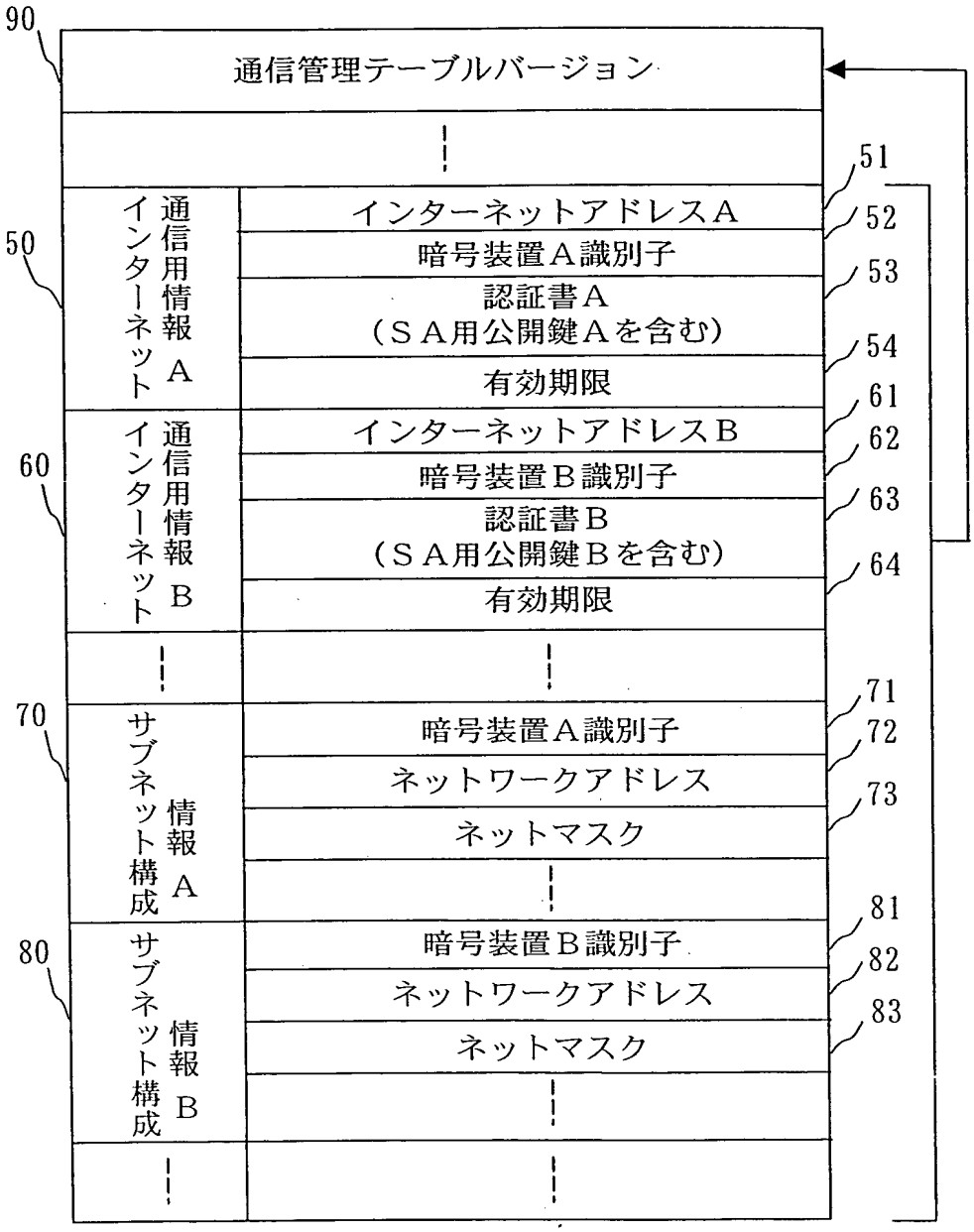

90
通信管理テーブルバージョン
50
通信用情報 インターネット A
51
インターネットアドレスA
52
暗号装置A識別子
53
認証書A
（SA用公開鍵Aを含む）
54
有効期限
60
通信用情報 インターネット B
61
インターネットアドレスB
62
暗号装置B識別子
63
認証書B
（SA用公開鍵Bを含む）
64
有効期限
70
サブネット構成情報 A
71
暗号装置A識別子
72
ネットワークアドレス
73
ネットマスク
80
サブネット構成情報 B
81
暗号装置B識別子
82
ネットワークアドレス
83
ネットマスク

図 8

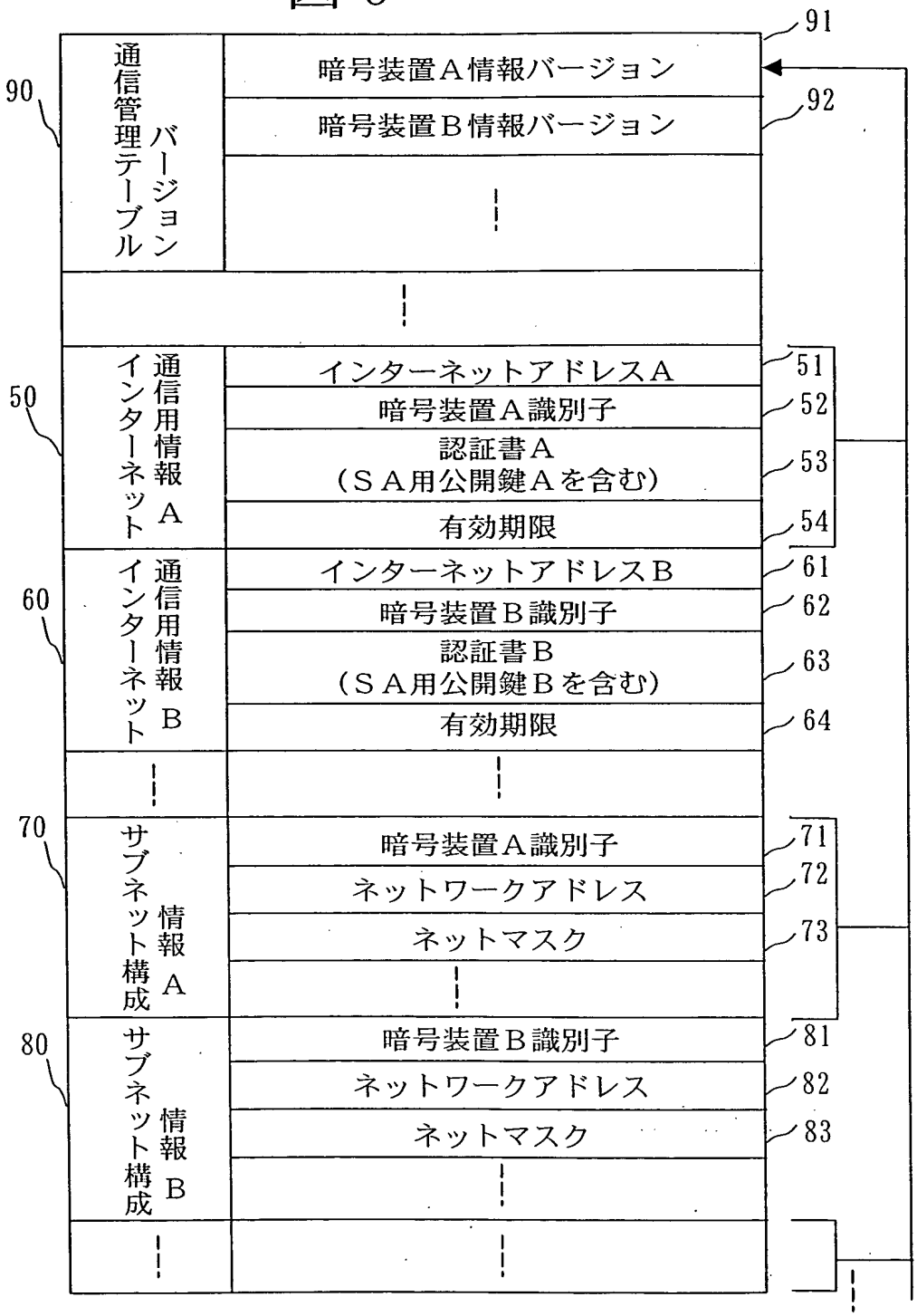

90
通信管理テーブル
バージョン
91
暗号装置Ａ情報バージョン
92
暗号装置Ｂ情報バージョン
50
通信用情報
インターネット
Ａ
インターネットアドレスＡ
51
暗号装置Ａ識別子
52
認証書Ａ
（ＳＡ用公開鍵Ａを含む）
53
有効期限
54
60
通信用情報
インターネット
Ｂ
インターネットアドレスＢ
61
暗号装置Ｂ識別子
62
認証書Ｂ
（ＳＡ用公開鍵Ｂを含む）
63
有効期限
64
70
サブネット構成
情報
Ａ
暗号装置Ａ識別子
71
ネットワークアドレス
72
ネットマスク
73
80
サブネット構成
情報
Ｂ
暗号装置Ｂ識別子
81
ネットワークアドレス
82
ネットマスク
83

図 9

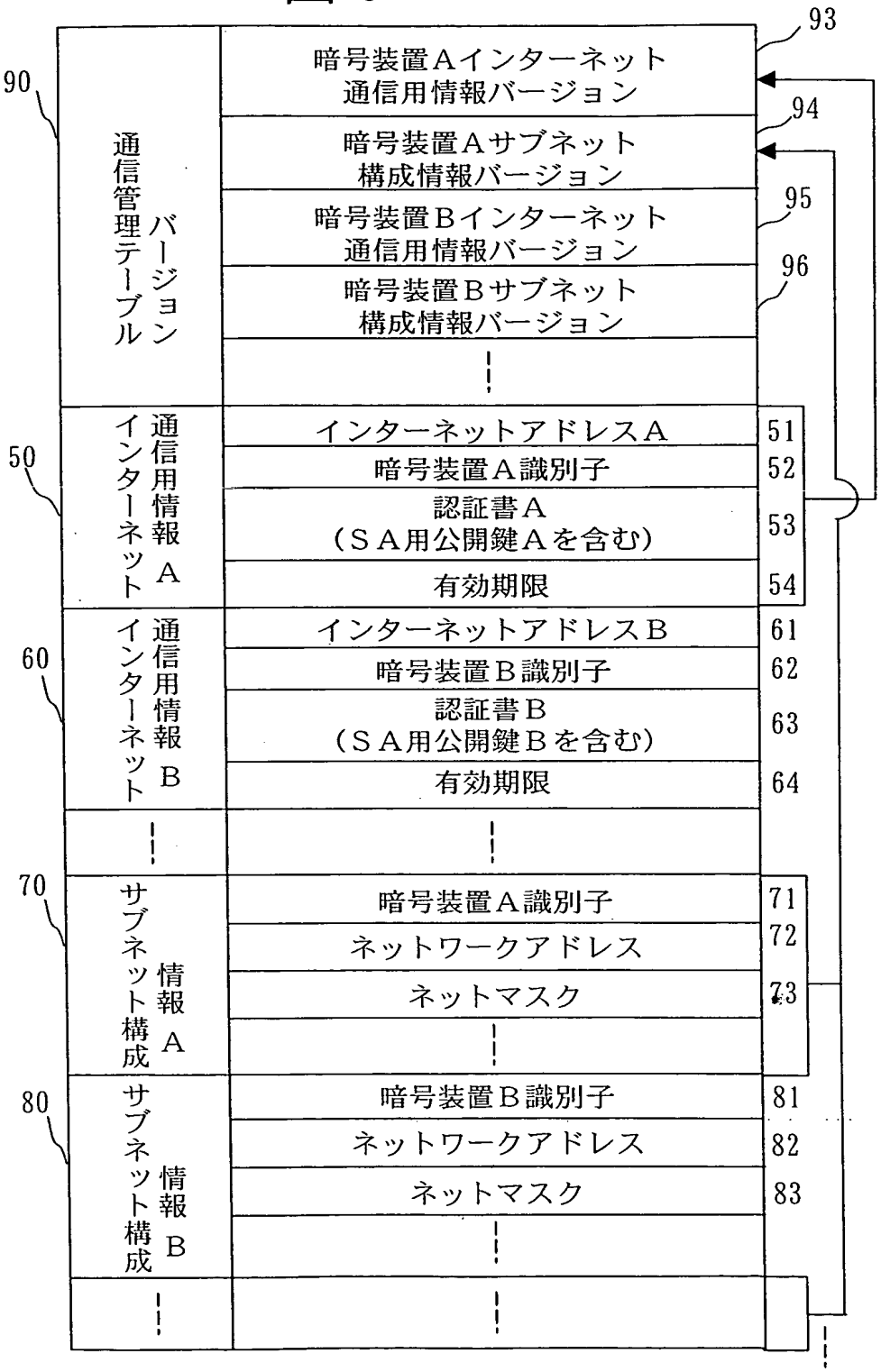

90
通信管理テーブル
バージョン
暗号装置Aインターネット通信用情報バージョン
暗号装置Aサブネット構成情報バージョン
暗号装置Bインターネット通信用情報バージョン
暗号装置Bサブネット構成情報バージョン
93
94
95
96
50
通信用情報インターネット A
インターネットアドレスA
暗号装置A識別子
認証書A（SA用公開鍵Aを含む）
有効期限
51
52
53
54
60
通信用情報インターネット B
インターネットアドレスB
暗号装置B識別子
認証書B（SA用公開鍵Bを含む）
有効期限
61
62
63
64
70
サブネット構成情報 A
暗号装置A識別子
ネットワークアドレス
ネットマスク
71
72
73
80
サブネット構成情報 B
暗号装置B識別子
ネットワークアドレス
ネットマスク
81
82
83

図 10

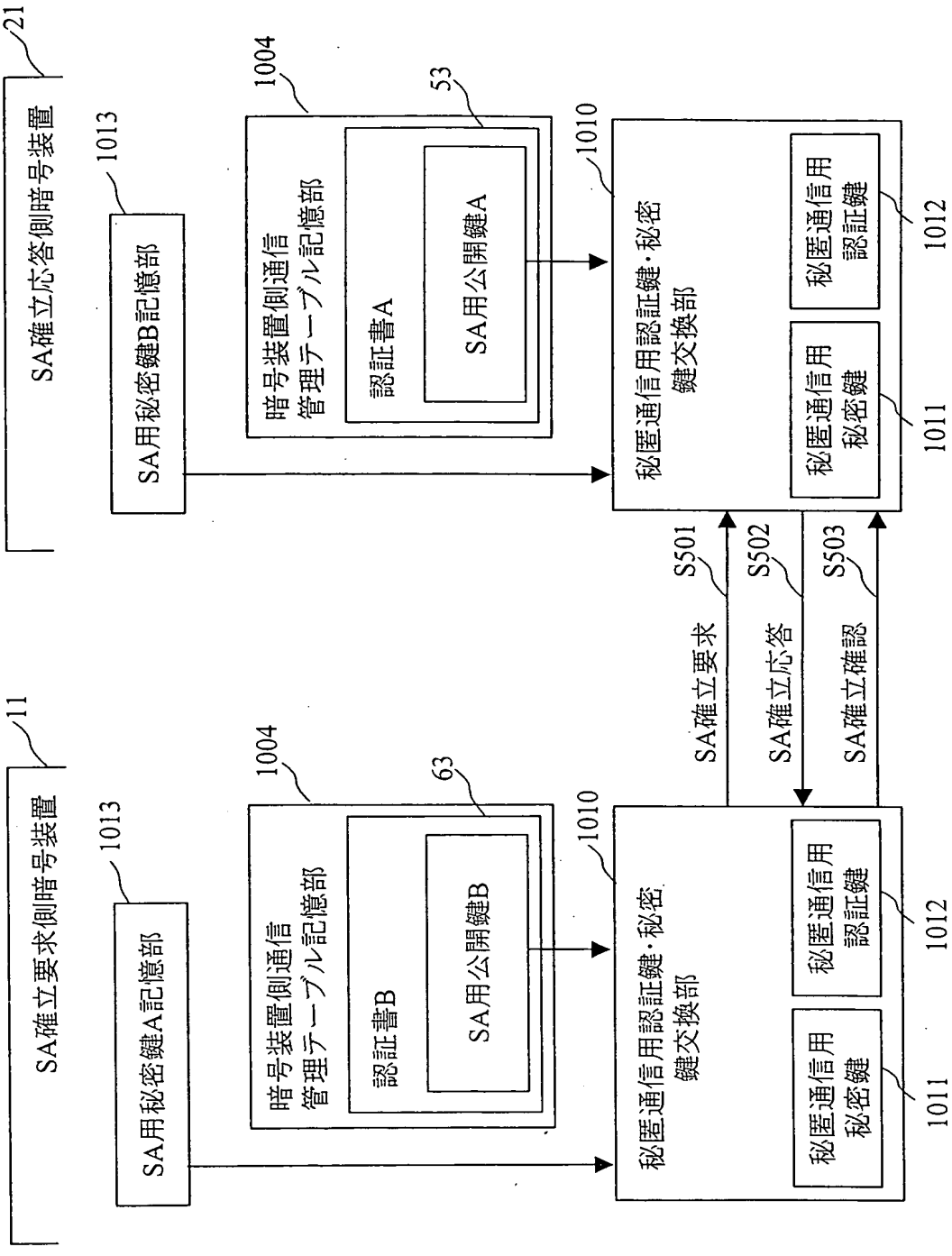

SA確立要求側暗号装置
11
SA用秘密鍵A記憶部
1013
暗号装置側通信
管理テーブル記憶部
1004
認証書B
63
SA用公開鍵B
秘匿通信用認証鍵・秘密
鍵交換部
1010
秘匿通信用
秘密鍵
1011
秘匿通信用
認証鍵
1012
SA確立応答側暗号装置
21
SA用秘密鍵B記憶部
1013
暗号装置側通信
管理テーブル記憶部
1004
認証書A
53
SA用公開鍵A
秘匿通信用認証鍵・秘密
鍵交換部
1010
秘匿通信用
秘密鍵
1011
秘匿通信用
認証鍵
1012
S501
SA確立要求
S502
SA確立応答
S503
SA確立確認

図 11

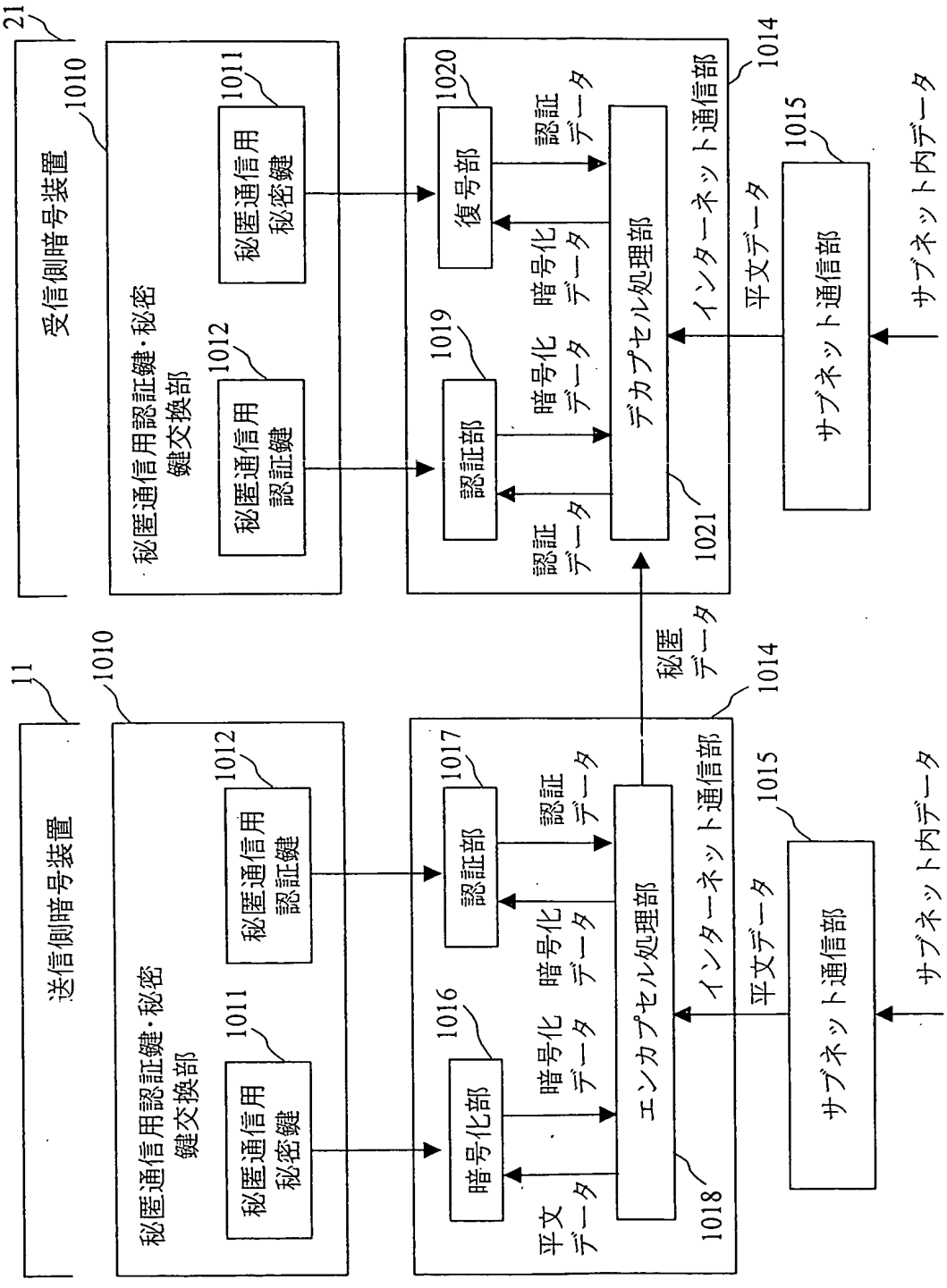

送信側暗号装置
11
秘匿通信用認証鍵・秘密鍵交換部
1010
秘匿通信用秘密鍵
1011
秘匿通信用認証鍵
1012
暗号化部
1016
認証部
1017
エンカプセル処理部
1018
インターネット通信部
1014
サブネット通信部
1015
サブネット内データ
平文データ
暗号化データ
認証データ
秘匿データ
平文データ
受信側暗号装置
21
秘匿通信用認証鍵・秘密鍵交換部
1010
秘匿通信用秘密鍵
1011
秘匿通信用認証鍵
1012
復号部
1020
認証部
1019
デカプセル処理部
1021
インターネット通信部
1014
サブネット通信部
1015
サブネット内データ
暗号化データ
認証データ
平文データ

図 12

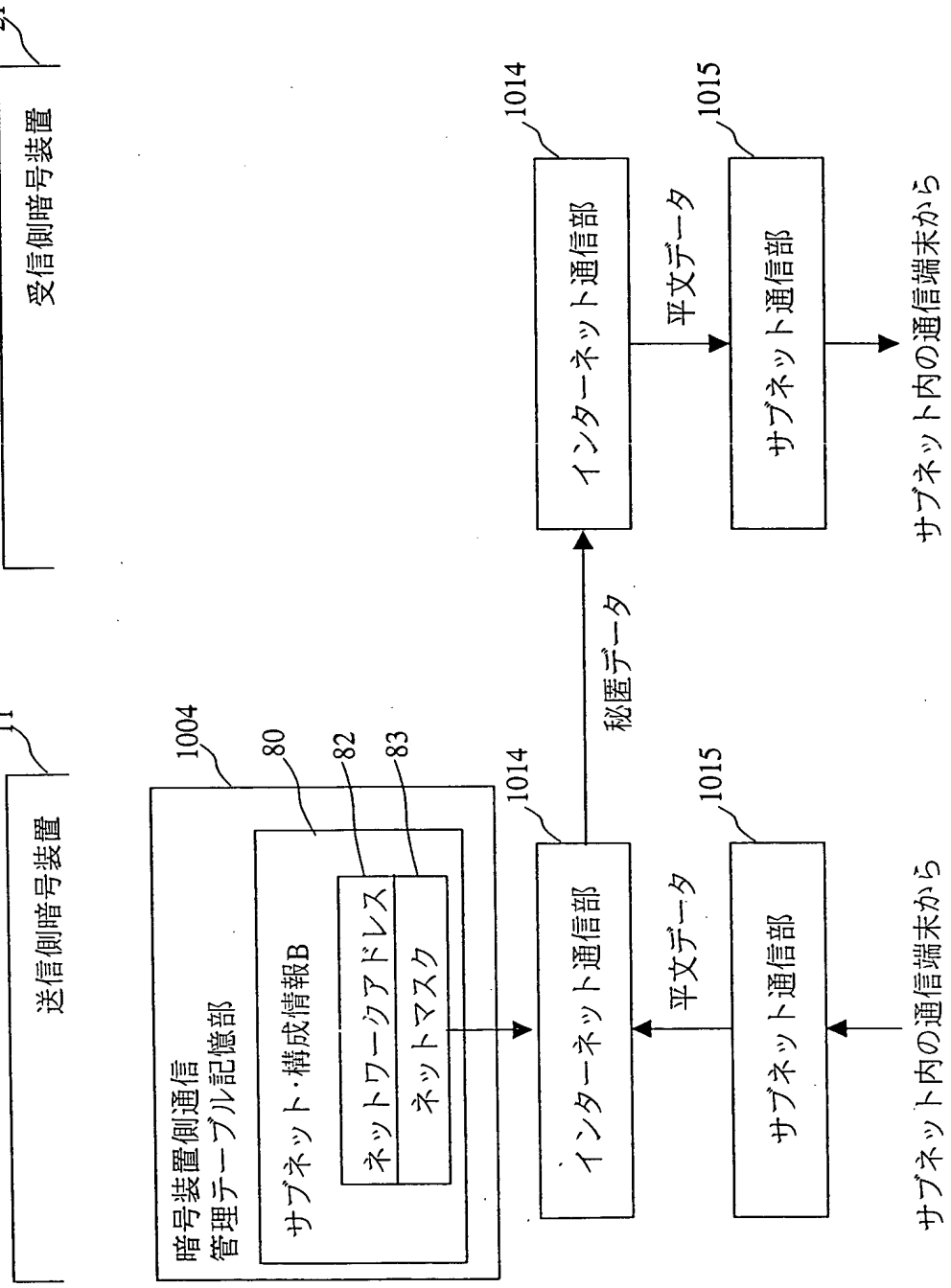

21
受信側暗号装置
1014
1015
インターネット通信部
平文データ
サブネット通信部
サブネット内の通信端末から
11
送信側暗号装置
1004
80
82
83
暗号装置側通信
管理テーブル記憶部
サブネット・構成情報B
ネットワークアドレス
ネットマスク
秘匿データ
1014
1015
インターネット通信部
平文データ
サブネット通信部
サブネット内の通信端末から

図 13

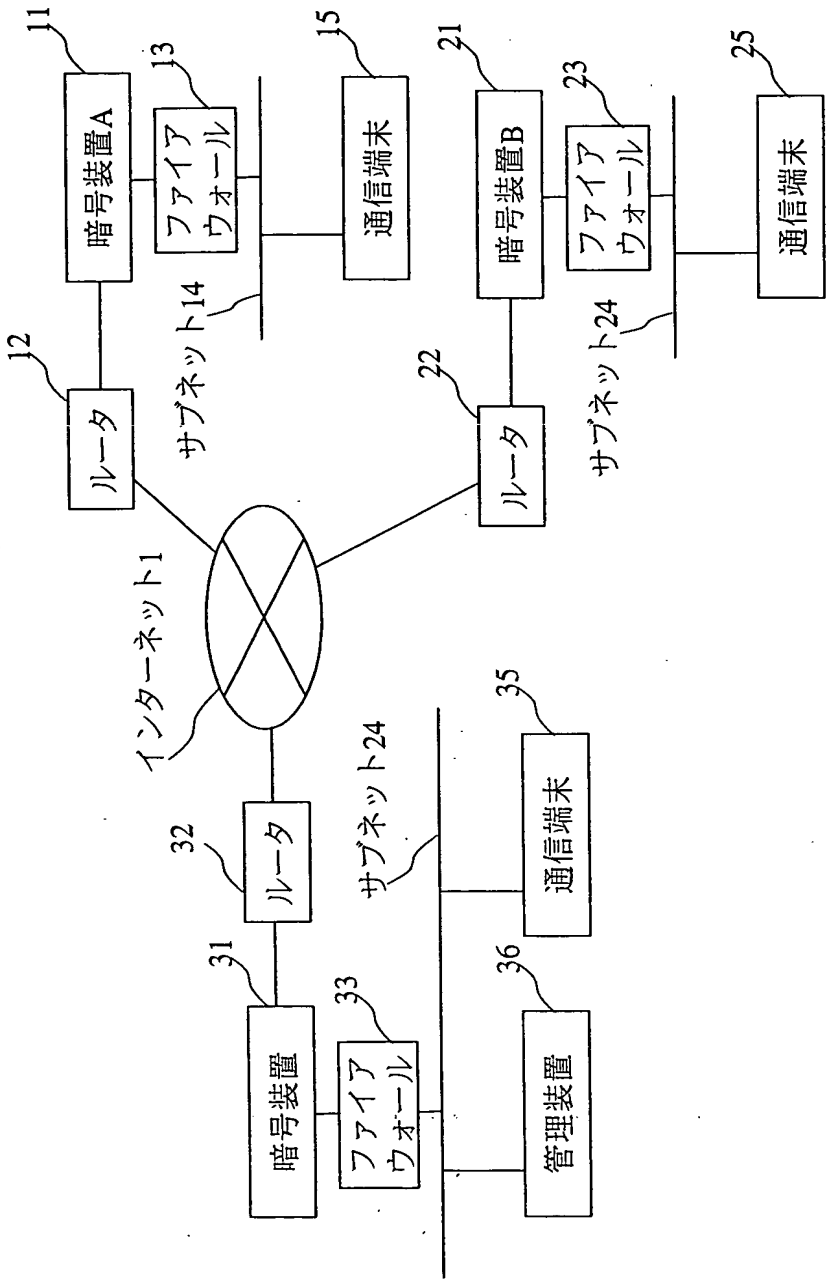

11
暗号装置A
13
ファイアウォール
15
通信端末
21
暗号装置B
23
ファイアウォール
25
通信端末
12
ルータ
サブネット14
22
ルータ
サブネット24
インターネット1
32
ルータ
サブネット24
35
通信端末
31
暗号装置
33
ファイアウォール
36
管理装置

図 14

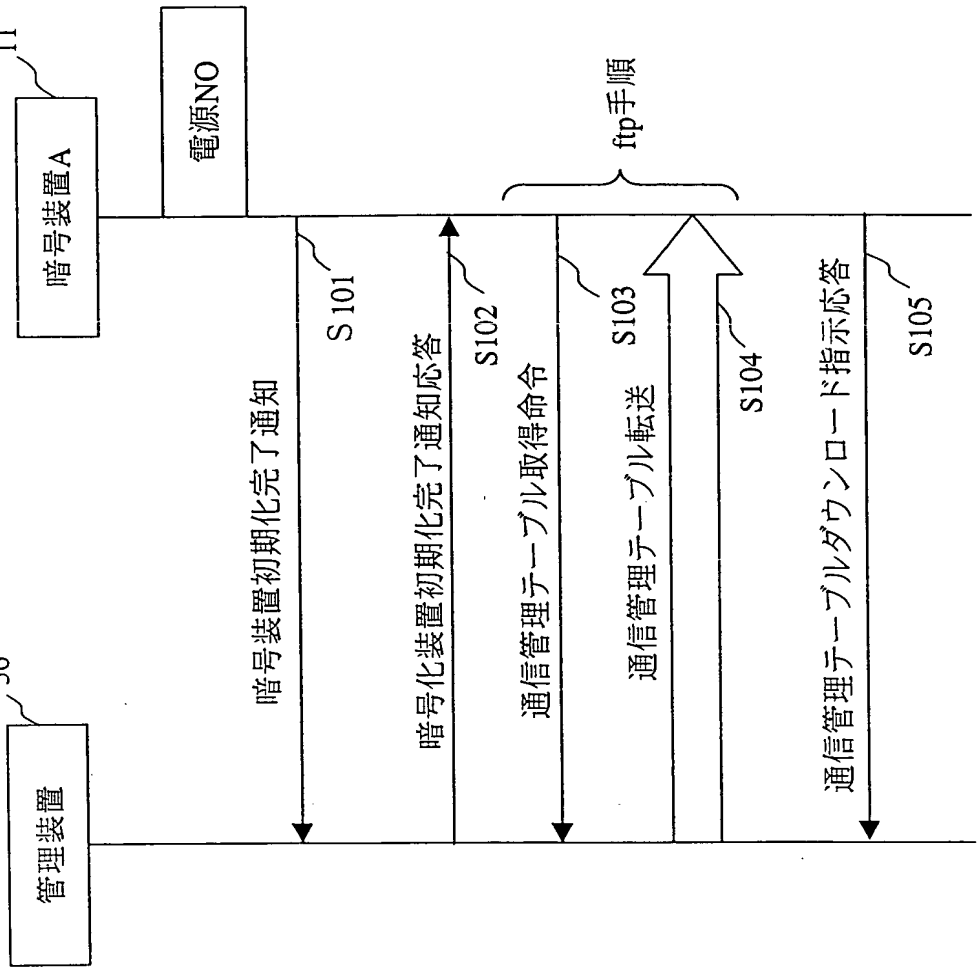
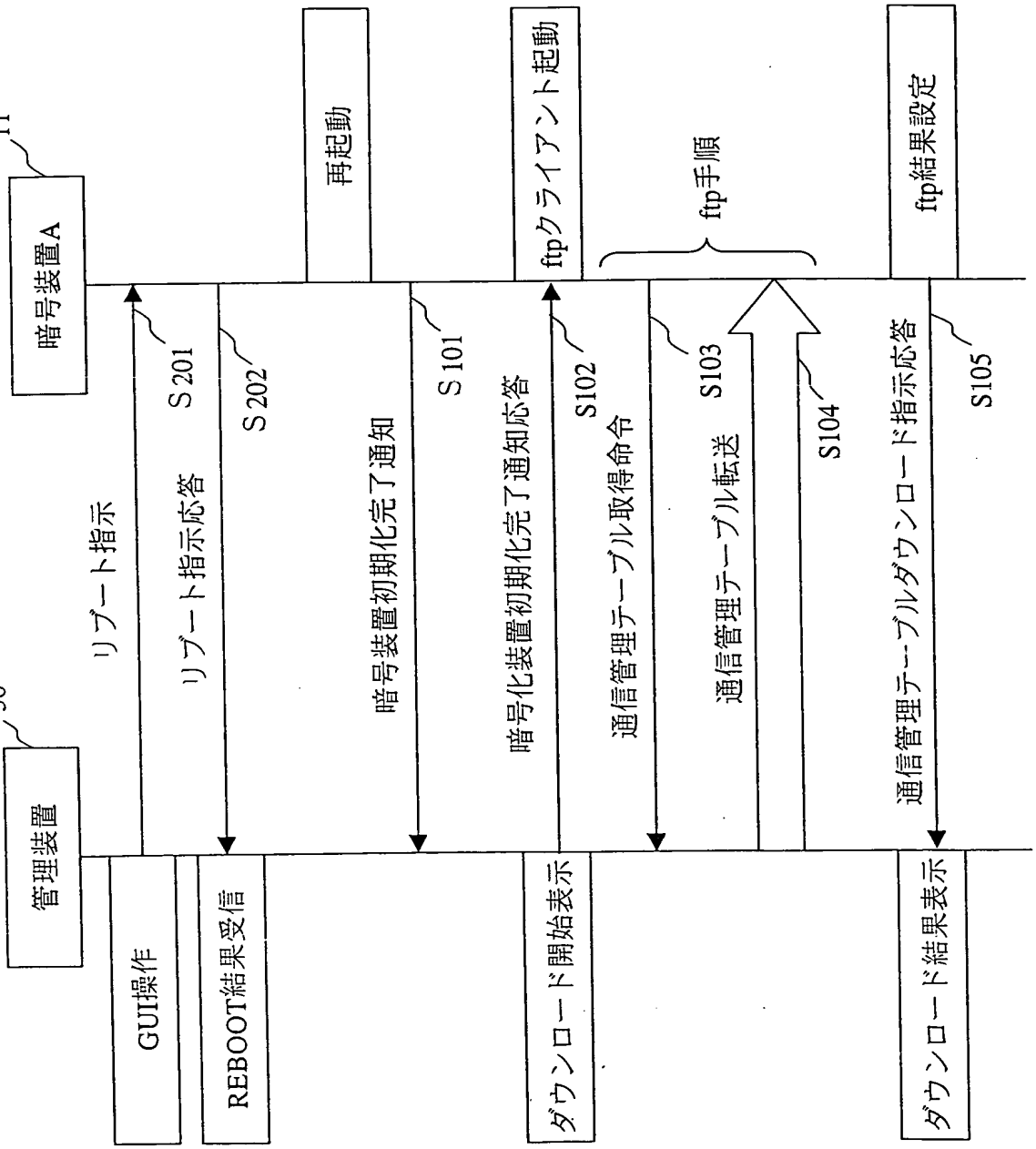

11
暗号装置A
電源NO
ftp手順
S101
暗号装置初期化完了通知
S102
暗号化装置初期化完了通知応答
S103
通信管理テーブル取得命令
S104
通信管理テーブル転送
S105
通信管理テーブルダウンロード指示応答
36
管理装置

図 15


11
暗号装置A
再起動
ftpクライアント起動
ftp手順
ftp結果設定
リブート指示
S201
リブート指示応答
S202
暗号装置初期化完了通知
S101
暗号化装置初期化完了通知応答
S102
通信管理テーブル取得命令
S103
通信管理テーブル転送
S104
通信管理テーブルダウンロード指示応答
S105
36
管理装置
GUI操作
REBOOT結果受信
ダウンロード開始表示
ダウンロード結果表示